

In The Matter Of:
United States vs.
PFC Bradley E. Manning

Vol. 21
July 25, 2013
UNOFFICIAL DRAFT - 07/25/13 Morning Session

Provided by Freedom of the Press Foundation

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

VOLUME XXI

IN THE UNITED STATES ARMY

UNITED STATES

VS.

MANNING, Bradley E., PFC. COURT-MARTIAL

U.S. Army, xxx-xx-9504

Headquarters and Headquarters Company,

U.S. Army Garrison,

Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

_____ /

The Hearing in the above-entitled matter

was continued on Thursday, July 25, 2013, at 9:30 a.m.,

at Fort Meade, Maryland, before the Honorable Colonel

Denise Lind, Judge.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

DISCLAIMER

This transcript was made by a court reporter who is not the official Government reporter, was not permitted to be in the actual courtroom where the proceedings took place, but in a media room listening to and watching live audio/video feed, not permitted to make an audio backup recording for editing purposes, and not having the ability to control the proceedings in order to produce an accurate verbatim transcript.

This unedited, uncertified draft transcript may contain court reporting outlines that are not translated, notes made by the reporter for editing purposes, misspelled terms and names, word combinations that do not make sense, and missing testimony or colloquy due to being inaudible by the reporter.

1 APPEARANCES:

2
3 ON BEHALF OF GOVERNMENT:

4 MAJOR ASHDEN FEIN

5 CAPTAIN JOSEPH MORROW

6 CAPTAIN ANGEL OVERGAARD

7 CAPTAIN ALEXANDER von Elten

8
9 ON BEHALF OF ACCUSED:

10 DAVID COOMBS

11 CAPTAIN JOSHUA TOOMAN

12 MAJOR THOMAS HURLEY

1 PROCEEDINGS

2 THE COURT: Court is called to order.

3 Major Fein, please account for the parties.

4 MAJOR FEIN: Yes, Your Honor. All parties

5 when the Court last recessed are again present.

6 Captain Morrow is present and Captain Whyte is absent.

7 Additionally, Your Honor, as of 9:20 this
8 morning, there are 54 members of the media at the Media
9 Operation Center, one stenographer, eight members of
10 the media in the courtroom in the panel box, 35
11 spectators in the courtroom and 14 spectators in the
12 overflow trailer.

13 Also, the alternate site other than the
14 chapel is available, if needed, because the overflow
15 trailer is not at maximum capacity, is not being
16 currently used.

17 THE COURT: All right. Thank you.

18 MAJOR FEIN: Also, the Court Reporter has
19 changed. Mr. Robert Shaw is absent. Mr. Chavez is
20 present.

21 THE COURT: All right. Have we had any

1 additional exhibits filed with the Court Reporter?

2 MAJOR FEIN: Yes, your Honor. Appellate
3 614, dated July 24, 2013, is a Defense motion for
4 reconsideration and for mistrial for Specification 4,
5 6, 8, 12 and 16 of Charge 2, 18 USC 641 offenses.

6 Gollihood 615, dated 25 July 2013, is a
7 Government accounting of expert witness for
8 presentencing.

9 Appellate Exhibit 616, dated 25 July 2013
10 is the Government's schedule of witnesses for
11 presentencing phase. And also, Your Honor, Appellate
12 Exhibit 617 is a Government's classified supplement for
13 closing argument.

14 THE COURT: What was 616 again?

15 MAJOR FEIN: Your Honor, United States
16 schedule or proposed schedule for sentencing witnesses.

17 THE COURT: Mr. Coombs.

18 MR. COOMBS: Yes, Ma'am. With regard 614
19 our motion, the Defense would request ability to
20 publish that motion today on its website. I believe in
21 accordance with the Court's requirements the motion can

1 be published. I know the Government has a process
2 which anytime there is an Appellate Exhibit, it
3 ultimately gets put on the FOIA reading room. However,
4 I would like to have the motion posted today.

5 THE COURT: Government, any objection?

6 MAJOR FEIN: Your Honor, so long as the
7 Court's Order is being followed, no objection.

8 THE COURT: All right. That's fine, Mr.
9 Coombs.

10 All right. The Court, once again, is
11 prepared to rule on the Defense motions for Finding of
12 Not Guilty under Rules of Court Martial 917. The Court
13 ruled on this yesterday actually and gave the parties
14 an advanced copy of the ruling so they would be
15 prepared, either in closing argument today.

16 Last night Mr. Coombs sent by email a copy
17 of the Request for Reconsideration that he has filed.
18 And before I read the ruling, counsel and I met briefly
19 in an RCM 802 conference before we came on the record
20 today.

21 Once again, that is a conference where the

1 parties and Court discuss logistics and scheduling and
2 other issues that might arise in cases.

3 The Government will file a response to that
4 motion by tomorrow evening. And over the weekend Mr.
5 Coombs will advise the Court on whether or not the
6 Defense request oral argument on that motion. And we
7 have not scheduled oral argument for it yet --
8 actually, we will. If we have oral argument on that
9 motion, it will be Monday morning 0930.

10 (The Court read ruling)

11 Is there anything else we need to address
12 before we proceed to closing argument?

13 MR. COOMBS: If we could have a brief
14 ten-minute conference break.

15 THE COURT: All right. Why don't we recess
16 the Court then until 10:45.

17 (Brief Recess)

18 THE COURT: Court is called to order.
19 Record reflect that all parties present when the Court
20 last recessed are again present.

21 Government, ready to proceed?

1 MAJOR FEIN: Yes, Your Honor.

2 Your Honor, if it may please the Court. In
3 late October 2009 Pfc.. Bradley Manning deployed with his
4 unit to a war zone, having sworn an oath of allegiance
5 in a place to protect national security interest of the
6 United States.

7 He deployed fully armed, not only with
8 protective gear and a rifle, but armed with the stark
9 knowledge of the harm that could accrue if classified
10 materials compromised.

11 His mission, as an all intelligence
12 analyst, was a special trust. But within weeks of
13 arriving at Iraq, he abused and destroyed this trust
14 with the wholesale, indiscriminate compromise of
15 hundreds of thousands of classified documents.

16 He delivered these documents ready made for
17 use by an enemy via a platform he had long researched
18 and come to know, WikiLeaks. He delivered these
19 documents for notoriety.

20 Pfc. Manning's state of mind has been
21 subject of speculation throughout this trial, Your

1 Honor. Yet human dog tags coupled with the fact of the
2 matter is that the only human Pfc. Manning ever actually
3 cared about was himself and his carelessness is
4 revealed through his own chats.

5 If at the country, he got notoriety.
6 Worldwide anarchy in CSD format Hillary Clinton is
7 going to have a heart attack. And the best evidence of
8 Pfc. Manning's state of mind before he had time to make
9 up a story is a picture, Your Honor. This picture, a
10 picture is worth a thousand words.

11 This picture was taken by Pfc. Manning
12 himself in January of 2010, during the same week he
13 transmitted hundreds of thousands of Significant
14 Activity Reports to WikiLeaks. And this picture, Your
15 Honor, was found in the same SD card as those
16 classified SigActs.

17 What you see, Your Honor, in this picture
18 is not a troubled, anguished or well intentioned
19 soldier struggling with the consequences of U.S.
20 military action or foreign policy. This is a gleeful,
21 grinning Pfc. Manning, who signed the transmittal letter

1 to WikiLeaks describing the SigActs with the
2 salutation, have a good day.

3 Pfc. Manning has been six months of a combat
4 deployment. Abusing his access is pertinent. Looking
5 for bigger fish, more damaging information to scrape
6 because he wasn't interested in oaths, or obligations,
7 or simple acknowledgments that he would protect closely
8 held information.

9 He was interested in making a name for
10 himself. A statement he made prior to deployment
11 turned out actually to be true. The flag meant nothing
12 to him.

13 Pfc. Manning was calculating and
14 self-interested. His acts resulted in the unfettered
15 access to classified information by enemies of the
16 United States, an outcome all too clear to him as a
17 result of his training, Your Honor.

18 How did Pfc. Manning know the enemy would
19 receive this information? He's aware of how WikiLeaks
20 operated and the type of information they sought. He
21 knew that what he provided to WikiLeaks would make its

1 way to the enemy. Because he knew the enemy used
2 WikiLeaks as their own resource. Pfc. Manning knew that
3 WikiLeaks, and specifically Julian Assange, considered
4 themselves the first intelligence agency for the
5 general public. Because it did, quote, from his chats
6 everything an intel agency does, end quote.

7 Pfc. Manning scoured every possible source
8 about WikiLeaks he could find on SIPRnet, the
9 classified SIPRnet, and saw how the United States
10 Government intelligence community considered WikiLeaks
11 a threat to the United States, an organization with the
12 term "leak" in their name who specialized in assisting
13 those with access to classified information and
14 extracting that information from Government systems and
15 disclosing it to the world anonymously.

16 Your Honor, there's voluminous amounts of
17 evidence in this case. And United States is cognizant
18 the clear understanding of what Pfc. Manning did or did
19 not do and what he did or did not know.

20 In order to best understand this complexity
21 of the evidence, the United States intends to follow

1 this roadmap for the remaining portion of the argument.

2 First, Your Honor, a recount of key
3 evidence. The United States intends to explain how Pfc.
4 Manning's formal education and training gave him skills
5 and knowledge that he ultimately used to the detriment
6 of the United States.

7 Then, Your Honor, I intend to explain Pfc.
8 Manning's work product as an intelligence analyst to
9 demonstrate how he knew and appreciated the types of
10 information he deliberately and intentionally chose to
11 compromise.

12 Then, Your Honor, I intend to explain Pfc.
13 Manning's actual knowledge of WikiLeaks through his own
14 words and research, focusing on what Pfc. Manning knew
15 and thought at the time he was actually compromising
16 information to WikiLeaks.

17 Then, Your Honor, I intend to walk you
18 through the evidence in a chronological order by type
19 of information that Pfc. Manning intentionally and
20 deliberately compromised through multiple
21 transmissions. This, Your Honor, is the order that you

1 will see.

2 Then, Your Honor, I'll outline the evidence
3 proving that Pfc. Manning wantonly caused intelligence
4 to be published on the internet, conduct that was
5 prejudicial to good order and discipline and services
6 discredit to the armed forces.

7 Finally, Your Honor, I'll outline the
8 evidence that will prove that Pfc. Manning aided the
9 enemy of the United States by knowingly giving
10 intelligence through indirect means to al-Qaida and
11 al-Qaida in the Arabian Peninsula.

12 Throughout this case, Your Honor, the
13 United States admitted more than 160 pieces of physical
14 and documentary evidence. The Court has heard
15 testimony from more than 80 witnesses, including
16 stipulations of expected testimony and two stipulations
17 of fact.

18 Although all this evidence is useful to
19 understand how Private First Class Manning committed
20 his crimes, as it relates to specific specifications
21 and charges that are key pieces of evidence for which

1 the United States explained during the opening that
2 spent more than one of the specifications. And the
3 United States argues that this evidence, this key
4 evidence, should remain in the forefront of your mind
5 during deliberations.

6 First, Your Honor, SIPRnet computers
7 identified as .22 and .40. These two SIPRnet computers
8 and the computers -- and it is his link to closely held
9 world maintained by an intelligence community on
10 SIPRnet.

11 Second, Pfc. Manning's personal computer, an
12 Apple McIntosh laptop. This computer was Pfc. Manning's
13 connection between the closely held war on SIPRnet and
14 his connection to the rest of the world. He used this
15 computer to communicate and transfer the closely held
16 information to Julian Assange, to WikiLeaks.

17 He also forensically wiped his computer on
18 31 January 2010, thus covering his tracks and deleting
19 any forensic evidence of his crimes prior to that date.

20 What Pfc. Manning did not plan for, Your
21 Honor, was the ability of the forensic examiners to

1 recover certain information such as the chats between
2 him, Julian Assange and Adrian Loma and the volume
3 mounting data.

4 The voluminous data shows the date that
5 certain information was burned on the CDs from his
6 SIPRnet computer and the CDs brought into and
7 introduced by his personal Mac. That information was
8 logged as a key piece of evidence in this case.

9 Third, Your Honor, Pfc. Manning's external
10 hard drive. This is an external storage device that he
11 brought to Iraq with him to store contact information
12 for WikiLeaks, army doctrine and training, his own
13 corrected training offset briefing, which I'll discuss
14 later.

15 Fourth, Pfc. Manning's SD card, on which he
16 saved a copy of the entire SigAct portion of CIDNI Iraq
17 and Afghanistan databases as a trophy for successful
18 disclosures.

19 Fifth, Jason Katz's computer from
20 Brookhaven National Laboratories, which contained the
21 Granai airstrike video compromised by Pfc. Manning in a

1 file dated 15 December, 2009. 15 December 2009, Your
2 Honor.

3 The sixth key piece of evidence are the
4 audit logs. These are from multiple servers, firewalls
5 operating on SIPRnet, which captured Pfc. Manning's
6 minute-by-minute activity across the classified web.
7 Intelink logs that show searches for WikiLeaks 119
8 times during 1 December 2009, two weeks, Your Honor,
9 after having access to SIPRnet.

10 The same time SharePoint server logs
11 showing the (inaudible) investigation being accessed.
12 Department of State server and firewall logs showing
13 amounts of data and activity in the late March and
14 early April 2010 timeframe. The Centaur net flow data
15 logs that show Pfc. Manning crisscrossing across the
16 SIPRnet connecting a different service to his two
17 SIPRnet computers.

18 Your Honor, seven, the computer with the IP
19 address ending .19. This is the computer Pfc. Manning
20 used to steal USF-I Global Access List.

21 The eighth piece of key evidence, Your

1 Honor, Prosecution Exhibit 130. Your Honor,
2 Prosecution Exhibit 130 is the evidence showing Pfc.
3 Manning elicited Julian Assange to assist him in
4 cracking a password, a user password on a SIPRnet
5 computer.

6 And finally, Your Honor the WikiLeaks Most
7 Wanted List, Pfc. Manning's guiding light on what
8 SIPRnet available information he should target for
9 release.

10 Your Honor, as previously stated, Pfc.
11 Manning is and was at the time an all source
12 intelligence analyst. He was granted SIPRnet access to
13 accomplish his duties and responsibilities as an
14 intelligence analyst.

15 He received a full complement of training
16 for 35 to AIT. Multiple witnesses testified that Pfc.
17 Manning was AIT, attended every class that they could
18 remember, received formal training presented in
19 Prosecution Exhibit 5 and Prosecution Exhibit 6. Your
20 Honor, those are the program instruction lesson plans
21 and AIT student evaluation plan.

1 Your Honor, in terms of information
2 security, specifically information security. Pfc.
3 Manning received a briefing that's at Prosecution
4 Exhibit 52. That's this slide. This is Slide 1. The
5 actual training Pfc. Manning received on information
6 security Army Regulation 380-5.

7 Slide 7, Your Honor, the classification
8 designations. What information was confidential,
9 secret, top secret, what does it mean when something is
10 secret or confidential. That it can cause serious
11 damage to national security.

12 Slide 8, Your Honor, the process of
13 classifying information. How do the United States
14 Government, under the Executive Order and Army
15 Regulations classify who are the proper authorities and
16 who is allowed to make those decisions.

17 Your Honor, Slide 10. The criterion
18 classified information. What type of information is
19 classified when you see a classified document from
20 military plans and weapon systems to foreign relations.

21 Slide 11, Your Honor, the prohibitions and

1 limitations. And the key here is in the blue on the
2 bottom where Pfc. Manning was put on notice that
3 classified information is owned by and produced by and
4 is under the control of the United States Government.

5 Your Honor, Slide 14, Pfc. Manning learned
6 how to properly mark documents and read documents and
7 know if they are marked classified.

8 Slide 21. He learned about the
9 declassification process; who are the authorities; who
10 is allowed to let information out of the possession of
11 the United States Government.

12 Slide 31. He specifically learned about
13 individual responsibility. His responsibility to
14 protect classified information.

15 Slide 38. The different way to store
16 classified information, the standards and regulation.

17 And Slide 41, the control measures in place
18 in order to protect classified information.

19 Your Honor, during the briefing he also
20 learned under Slide 48 how to properly mark digital
21 media with the different types of stickers, if it's

1 secret, top secret, unclassified or confidential.

2 We know Pfc. Manning understood how to label
3 digital media in this case. You heard Special Agent
4 Smith that he found the Apache video on a disk in Pfc.
5 Manning's shoe on a secret sticker. This is it, Your
6 Honor, Prosecution Exhibit 15. A secret sticker that
7 Pfc. Manning put on the CD because he believed at the
8 time, even though he burned it from his personal
9 McIntosh computer, that that video, the Apache video
10 was classified secret.

11 Your Honor, according to Prosecution
12 Exhibit 52, Private First Class Manning was trained
13 also on why it was important to protect particular
14 information. So here is Slide 71. The enemy will
15 attempt to discover how and when we are conducting
16 operations. Knowing this we must protect our
17 activities from detection.

18 Slide 72. The critical information we
19 protect from enemies. (Inaudible)

20 Finally, Your Honor, Slide 73. The reason
21 we prevent disclosures in bright bold red. Don't

1 discuss operational activities on the web or email.
2 Consider the audience when you are posting to a blog,
3 personal web page or an email. Always assume the
4 adversary is reading your material. And at bottom,
5 remember, it's called the worldwide web for a reason.

6 This is the training he received day one as
7 an intelligence analyst.

8 What slide you did not see in the slide
9 deck presented in Prosecution Exhibit 52 for the entire
10 set of slides, the slide that tells Pfc. Manning that
11 he's authorized to make classification decisions. He's
12 authorized to disclose information he chooses to, to
13 foreign nationals and ultimately to enemies of the
14 United States.

15 Your Honor, Mr. Moul, Pfc. Manning's AIT
16 instructor recounted that, when instructing Pfc. Manning
17 in his class, he explained that the worldwide web was
18 called that for a reason. Anyone had access to the
19 information on the internet and can see any of the
20 information that is on the internet. It was imperative
21 that soldiers understood this.

1 Mr. Moul taught Pfc. Manning that whenever
2 they put information on the internet that it could be
3 used against them or against the U.S. military. And he
4 talked the following example, his own words, to the
5 lowest level of how posting information, how it could
6 help the enemy, if given soldier's name, mother's
7 maiden name and social security number, filed separate
8 as an example couldn't do much damage.

9 But he explained to the lowest level, when
10 that information is combined, and that is put on the
11 internet, that a person could grab that information,
12 take credit out of someone's name and do harm to that
13 individual and that individual's reputation.

14 Similarly, he taught Pfc. Manning, if you
15 release a unit's name, their location and mission, then
16 the enemy can use that information to plan an attack on
17 our units.

18 Your Honor, Pfc. Manning was trained on the
19 identities of terrorist groups, including al-Qaida,
20 using training slides from AIT, Prosecution Exhibit 51,
21 Mr. Moul testified that Pfc. Manning was trained the

1 enemy used the internet. And that anything that the
2 enemy can use or piece together to use against the
3 United States should be protected, to include PPI, unit
4 identification and movement information.

5 Mr. Moul also instructed Pfc. Manning on
6 specific enemies and what capabilities. He taught Pfc.
7 Manning about terrorism and different terrorist
8 organizations.

9 Slide 216, Your Honor, Pfc. Manning formally
10 learned who al-Qaida was and specifically who Osama bin
11 Laden was.

12 Slide 219, formally learned who al-Qaida in
13 Iraq was. Slide 221, learned about the recruiting that
14 terrorists did.

15 Slide 223, Pfc. Manning learned that over
16 the past 10 years the number of terrorist websites has
17 jumped from less than 100 to as many as 4,000.

18 In addition to this training, Your Honor,
19 the United States admitted Pfc. Manning's information
20 assurance training and certificates that showed he
21 completed that training. Prosecution Exhibit 7 and

1 Prosecution Exhibit 114.

2 Your Honor, Prosecution Exhibit 7 the
3 training that he received in 2008 and 2009. Slide 2,
4 based off this training he knew each and every one of
5 us play a vital role in DoD information safe and must
6 abide by the principles of IA in a daily routine and
7 protect the OB information in our systems.

8 Your Honor, Slide 7 of the training that he
9 passed the test twice on. Pfc. Manning knew the
10 importance of critical infrastructure protection, that
11 if information and information systems are compromised,
12 it can impact our mission or national security and
13 ultimately our lives.

14 Your Honor, Slide 11. Prosecution Exhibit
15 7. Pfc. Manning knew the threats made to information
16 assurance, which included both internal and personal
17 human threats, specifically disgruntled employees,
18 spies or terrorists and hackers.

19 Your Honor, as a trained intelligence
20 analyst, Pfc. Manning was required to have a secret
21 clearance AIT and eventually top secret SCI clearance

1 as a full 35 Fox.

2 Pfc. Manning knew that a person may only be
3 granted access to classified information if three
4 things were true; first, the individual has a security
5 clearance; two, individual has a need to know the
6 information; and three, the person has signed a
7 nondisclosure agreement, SF312.

8 Pfc. Manning signed on two separate
9 nondisclosure agreements and a litany of other
10 acknowledgments. These documents permitted him to have
11 access to classified information, identified the
12 information that was owned by the United States
13 Government, highlighted potential ramification to
14 disclose or handle classified information improperly
15 and what a soldier is required to do if he is uncertain
16 of the classification status of the information. A
17 document signed, two documents, signed by Pfc. Manning
18 on what he is required to do, if he's uncertain about
19 classification.

20 A violation of nondisclosure agreements can
21 result in criminal prosecution under 18 U.S.C. 7-903

1 and 641.

2 Your Honor, Elisa Ivory, she testified
3 through a stipulation of expected testimony that on 7
4 April, 2008, she briefed Pfc. Manning about the dangers
5 of putting U.S. Army and Government classified
6 information on the internet.

7 She briefed Pfc. Manning that putting
8 information on the internet not only exposes
9 information related to our national security, but it
10 also puts each soldier with a security clearance at
11 risk of blackmail by our adversaries given their
12 position of trust to safeguard classified information.

13 Ms. Ivory also explained to Pfc. Manning the
14 purpose of the NDA. And it asked Pfc. Manning if he
15 wanted to voluntarily sign that. He did. Then Pfc.
16 Manning stood, raised his right hand and stated that he
17 accepted the responsibilities contained within that
18 nondisclosure agreement. Including that he accepted
19 the special confidence and trust placed in him by
20 United States Government. Pfc. Manning then executed
21 that NDA with Ms. Ivory.

1 Prosecution Exhibit 59 is that
2 nondisclosure agreement, which Pfc. Manning pledged not
3 to violate in order to obtain access to classified
4 information.

5 Now, Your Honor, Prosecution Exhibit 60 is
6 a second nondisclosure agreement, which Pfc. Manning
7 pledged not to violate in order to obtain classified
8 information while at 210 Mountain. And Chief Balonek
9 made sure he understood those obligations, as he
10 testified.

11 Your Honor, by voluntarily signing two
12 nondisclosure agreements, he knew the importance of
13 protecting classified information and that the
14 violations of the agreements could result in the
15 precise criminal action of this trial.

16 Pfc. Manning knowingly violated both
17 nondisclosure agreements; thus, violating the special
18 trust and confidence that he committed to in order to
19 obtain access to classified information. That same
20 access that he abused in order to disclose hundreds of
21 thousands of classified documents.

1 Your Honor, during AIT Pfc. Manning learned
2 and understood how the United States Army and its
3 enemies waged war. This is evidenced by the amount of
4 training materials that Pfc. Manning himself retained
5 and cataloged on his external hard drive, Prosecution
6 Exhibit 11.

7 Your Honor, what did Pfc. Manning keep for
8 easy reference next to the WikiLeaks contact
9 information file, that's Prosecution Exhibit 24, talk
10 about a moment.

11 He kept the Microsoft PowerPoint Brief
12 Title Insurgent Propaganda TTPs. He kept a copy of
13 U.S. Army Field Manual 2-0 titled Intelligence, which
14 states that our enemies weapons range from computers
15 connected to the internet to weapons of mass
16 destruction.

17 He kept a copy of Army Regulation 525-13
18 entitled Anti-Terrorism. That regulation states that
19 terrorists use instances of website tampering to
20 further their cause.

21 He kept on his external hard drive a copy

1 of U.S. Army Field Manual 7-100.1, which states that
2 personal computers on the internet are few examples,
3 just a few, of the capabilities widely available to
4 nations, independent organizations and individuals.
5 Met the information warfare could be conducted with
6 such easily accessible means such as the internet.

7 He also kept a copy of Army field Manual
8 7-100.4, which in Appendix C states, that the insurgent
9 organizations may be capable of cyber mining for
10 intelligence.

11 Your Honor, Pfc. Manning neatly organized
12 possession of all this information on his external
13 hard drive. That is additional evidence he knew and
14 understood all that information.

15 He showed that he had actual knowledge by
16 enabling closely held information, information he
17 posted on the internet. He was given that information
18 that enemies of United States and specifically al-Qaida
19 and al-Qaida in the Arabian Peninsula.

20 In addition to AIT training and reference
21 material Pfc. Manning saved on his external hard drive,

1 he received formal and on-the-job training as an
2 intelligence analyst.

3 Your Honor, according to Sergeant First
4 Class Ehresman at his first JRTC rotation, Pfc.
5 Manning's job was focused on signature activities in
6 areas of operations. This required constant research,
7 constant reviewing of information related to attacks
8 that insurgents were conducting, such as with IEDs,
9 small arms fire, indirect fire.

10 Pfc. Manning was required to pull that
11 information and put together timelines for the S2 shot,
12 when IEDs were occurring and how often and where. So
13 the other analysts could go patten analyses product to
14 see if the IEDs could be targeted.

15 The intelligence Pfc. Manning mined was
16 actually SigActs. Chief Balonek also testified he
17 trained Pfc. Manning on how to use D6A machine in data
18 mining. Chief Balonek testified that he worked with
19 Pfc. Manning on intelligence summaries of the day, which
20 were a daily rule of all the intelligence reporting
21 from that day compiled into one document. And each

1 analyst, like Pfc. Manning, was required to actually tag
2 it and give the meaning of those reports.

3 Your Honor, Mr. Madaras, then Sgt. Madaras,
4 testified that at his D6A training, Pfc. Manning was
5 told that D6A field support representative would be
6 downrange and be responsible for handling all hardware
7 and all software issues for the D6A machines in
8 theater. That is when Pfc. Manning was first put on
9 notice that the D6A contractors were in charge of those
10 computers.

11 Sergeant First Class Anika testified Pfc.
12 Manning had exposure to SigAct at Ft. Drum, not just at
13 JRTC. He is required to read reports, pick up the
14 highlights, locate the bad guys and brief those
15 findings to the S2 and ultimately to the brigade
16 commander, Colonel Miller.

17 Sergeant first-class Anika testified that
18 Pfc. Manning also read many intelligence summaries,
19 which included SigActs from the CIDNE database,
20 particular view from borne IED, assessment on pattern
21 analysis, assessments of the enemy in the area,

1 political figures that were friendly.

2 He also testified that the unit received
3 formal IED training in December of 2008. A mobile
4 training team, Your Honor, from the joint IED defeat
5 organization came to Ft. Drum to teach the analysts
6 what their organization did for units downrange and
7 where to go for assistance when finding IED cells in
8 certain area.

9 According to Mr. Madaras the unit trained
10 again in approximately July of 2009, at this time the
11 focus was on Iraq. During this second rotation Pfc.
12 Manning was, again, assigned to fusion cell and similar
13 responsibilities as the previous JRTC.

14 Your Honor, it's clear that Pfc. Manning
15 arrived at FOB Hammer with specialized training from
16 AIT, experience from two JRTC rotations and his
17 garrison intelligence work. He also arrived with an
18 external hard drive full of valuable and informative
19 intelligence references.

20 All this combined, Your Honor, all this
21 combined is enough to prove that Pfc. Manning's actual

1 knowledge that the enemies of the United States used
2 the internet and WikiLeaks to gather information to be
3 used against this country.

4 However, Your Honor, there is one key piece
5 of evidence which Pfc. Manning also brought to Iraq with
6 him that proves he should be held accountable for
7 deliberate and intentional acts of releasing volumes of
8 classified information through WikiLeaks to enemies of
9 this country.

10 We are here today, Your Honor, to hold Pfc.
11 Manning accountable for the exact training he gave
12 others, the training he gave others on this subject
13 matter.

14 During Mr. Johnson's forensic examination
15 of Pfc. Manning's external hard drive, he found Pfc.
16 Manning's corrective training presentation, which
17 Sergeant Madrid confirmed was the one presented to him
18 by Pfc. Manning. Your Honor, this is Prosecution
19 Exhibit 25.

20 Prosecution Exhibit 25, Slide 1, dated 13
21 June 2008, created, researched by, well then, Pv2

1 Manning, Bradley.

2 Your Honor, Slide 2, provides a roadmap to
3 protecting this country's operational security. Slide
4 3, Your Honor, Pfc. Manning's definition of OPSEC
5 focused on the protection of information, public
6 assets, military assets, personnel and national
7 security.

8 Slide 4, Your Honor, the type of
9 information to protect to include dates, times,
10 locations along also for official use only information,
11 such as the Army's capabilities on the battlefield.

12 Your Honor, Slide 5 of Pfc. Manning's own
13 briefing where he's highlighting that you must protect
14 dates and kind of large groups within the Department of
15 Defense, high ranking NCOs, and even diplomats, protect
16 their information, Your Honor.

17 Slide 6, protecting location of Government
18 facilities and military installations. Slide 7.
19 Protecting individual soldiers' names, family members,
20 dates of birth and addresses.

21 He recognized, Your Honor, that in Slide 7

1 soldiers are required to protect the names and other
2 identifying information of our fellow soldiers.

3 Slide 8. That we must protect the methods
4 of intelligence gathering, description of weapons and
5 vehicles we use, and the capabilities of the United
6 States Army.

7 9, Pfc. Manning specifically lists those
8 groups that he didn't consider adversaries of the
9 United States for the purpose of divulging closely held
10 information, foreign governments, terrorists and anyone
11 including activists and hackers.

12 Slide 10, Your Honor. On 13 June 2008,
13 after identifying the adversaries to the United States
14 Pfc. Manning further delineated the common OPSEC leaks
15 for closely held information. That includes on
16 newspapers and magazines, news programs and
17 documentaries and the internet. Including chatrooms,
18 social networking and videos.

19 And then on Slide 11, Your Honor, his
20 conclusion on 13 June, 2008, he concluded his briefing
21 by stating, soldiers must avoid disclosures of

1 information the following forums; public conversations
2 with journalists, posting information on the internet.
3 Soldiers must use common sense with OPSEC and protect
4 our nation's secrets. Because there are many enemies
5 and we live in a free and open society.

6 Your Honor, this is not the product of just
7 any soldier in uniform, but of Pfc. Manning, a trained
8 intelligence analyst who, on 13 June 2008, understood
9 what he taught others that the importance of protecting
10 our closely held information and knew that releasing
11 such information on the internet would be in the hands
12 of terrorists and other adversaries of this nation.

13 Your Honor, Pfc. Manning was an intelligence
14 analyst, as you know, assigned to the S2 Section at 210
15 Mountain. At FOB Hammer S2 Section worked in a T-SCIF
16 located in the brigade headquarter's building. The
17 T-SCIF was a facility designed to store classified
18 information.

19 Everyone who worked the T-SCIF was required
20 to have a top secret clearance. For requested access
21 required to have an escort to enter the SCIF. That

1 even included the brigade commander, Colonel Miller.

2 If the soldier did not have a security
3 clearance, the T-SCIF would be sanitized, each S2
4 soldier, including Pfc. Manning, was responsible for
5 moving classified information out of sight.

6 When a soldier entered or left the T-SCIF,
7 they are not searched. Instead it was their personal
8 responsibility to leave any electronic devices outside
9 the SCIF and not to remove any classified information
10 from the SCIF unless for official purposes only.

11 Your Honor, why were soldiers not searched?
12 Captain Lim gave that answer. He testified with the S2
13 section trust, trust was imperative because the
14 intelligence soldiers dealt with classified information
15 on a daily basis and it was their job, their specific
16 job to protect classified information.

17 Colonel (inaudible) testified that trust
18 within a unit is everything. It is no different as an
19 infantryman to trust another soldier to provide front,
20 rear and side security on a convoy, as it is for an
21 intelligence analyst who trusts his fellow analysts to

1 safeguard classified information from the hands of the
2 enemy.

3 If Pfc. Manning had not signed those NDAs
4 before he was deployed, he would not have worked in a
5 T-SCIF and would not have been able to commit the
6 crimes we are here today for.

7 Your Honor, you have heard from a number of
8 witnesses about the jobs of an intelligence analyst in
9 deployed environment. In Pfc. Manning's unit discussed
10 what systems were used, how intelligence products were
11 created and how to defeat the enemy, and what role Pfc.
12 Manning specifically played in that process.

13 Your Honor, first, let's talk about what
14 system the analyst used at FOB Hammer. Intelligence
15 analysts at FOB Hammer primarily used the SIPRnet to
16 gather intelligence.

17 From SIPRnet the analysts were assigned a
18 D6A computer system, get programs D6A computers
19 contained program that were regularly used by the
20 analysts and readily accessible a special suite of
21 programs installed in the SIPRnet computers designed

1 for United States Army all source intelligence analyst
2 to complete their assigned task.

3 Your Honor, you heard from Sergeant Sadler,
4 a SIGIT solider, not an all source intelligence
5 solider, who never even that was a system solely for
6 all source intelligence analyst.

7 Mr. Kits testified that the D6A machine is
8 essentially for intelligence processing and
9 exploitation and dissemination capabilities. Members
10 of S2 section had complied with the programs commonly
11 employed by analysts within the office were CIDNE
12 (inaudible)

13 (inaudible) Your Honor, commonly used
14 system and database for analysts. In particular
15 analysts regularly SigActs which are tactical reports
16 significant activity from the field.

17 Your Honor, Mr. Buchannon, through a
18 stipulation of expected testimony testified that
19 Intelink is a search engine on SIPRnet similar to
20 Google, that also enables collaboration among members
21 of the intelligence community.

1 Mr. Madaras explained that analysts
2 typically used Intelink when they didn't have specific
3 background knowledge on a certain topic so they didn't
4 know what database to go to originally. So they would
5 search on Intelink.

6 Analysts also used other programs, such as
7 mIRC chat, which is a collaboration tool, similar to
8 instant messaging, which allows analysts to quickly
9 receive and disseminate information to and from the
10 field up and down from the division to battalion.

11 Your Honor, you heard testimony how
12 analysts create their products and Pfc. Manning's role
13 in that process. Pfc. Manning was assigned to the
14 fusion cell at FOG Hammer where he was responsible for
15 contributing to the large scale enemy trained analysis
16 and predictive analysis focused on the Shia, his focus
17 in Southeast Baghdad Shia --

18 Your Honor, before continuing about the
19 steps that Pfc. Manning went through in order to
20 accomplish his normal intelligence and show his
21 knowledge of what intelligence analysts knew about the

1 enemy, please note that the suite of tools that the
2 Army gave Pfc. Manning to enable him to collate data,
3 those tools, that based on Pfc. Manning's actions he
4 enabled the enemy to have that information that the
5 United States relies on its special tools to collate,
6 organize and analyze.

7 He provided that information, packaged to
8 the enemy. So now they can just analyze. He took all
9 of the initial steps that they would need to do and
10 gave that to them packaged, ready to be exploited, and
11 the entire world. Yet we, United States Army, has
12 special systems that allows to pull that information.

13 So speaking of those systems, Your Honor,
14 the first step in the process is to pull and
15 consolidate from various sources a particular topic,
16 such as enemy activity in a region over a certain
17 period of time.

18 After organizing the information the
19 analysts would then plot the information on a map to
20 visualize or create an intelligence summary.

21 Members of Pfc. Manning's unit testified

1 that he was the go-to-guy for data mining, the process
2 of gathering mass intelligence on a particular topic
3 and organizing that intelligence in a usable format.

4 Pfc. Manning's job was to reach into foreign
5 databases, pull and organize it. He was ranked 10 out
6 of 10 in data mining. Captain Fulton and Chief
7 (inaudible) they testified in conducting this analysis
8 generally required (inaudible) to come databases for
9 the applicable SigActs.

10 Captain Fulton testified that often
11 employed Pfc. Manning to data mine for mass information,
12 particularly the SigActs relating to specific enemy
13 activity, organize and display it on a map for her.

14 The purpose of this task, as Captain Fulton
15 explained, was to determine whether the amount of
16 attacks had increased or decreased over a time, as the
17 unit prepared to draw down and redeploy from Iraq.
18 Fulton used this information to brief Colonel Miller on
19 a weekly basis to make command decisions.

20 Chief (inaudible) testified that Pfc.
21 Manning employed similar skills, so much so that he

1 prepared Iraq SigActs spanning a three year period in
2 IEDs, small arms fire against convoys and their
3 brigade.

4 The second step in this intelligence
5 analyst product, process. As Chief Ehresman explained,
6 was to make an assessment on the current inbound threat
7 or may happen in the immediate or distant future. The
8 second step is where the analysis comes into play;
9 mainly enemy trend analysis and predictive analysis.

10 Enemy trend analysis is a study of how our
11 enemies operate, to identify any trends or patterns in
12 their behavior. Predictive analysis is the art of
13 predicting enemy activity, enemy activity based upon
14 enemy trends. Or put another way, enemy trend analysis
15 leads to predictive analysis.

16 Chief Ehresman testified that historical
17 and current data are important for conducting this
18 analysis, as enemy groups tend to operate in the same
19 areas and employ the same tactics over time.
20 Historical information is just as useful intelligence
21 analyst as the most current information.

1 It benefits -- it benefit, the historic
2 information versus current, varies based of the desired
3 intelligence product. The focus of the product.

4 Both enemy trend analysis and predictive
5 analysis is essential for the commander to make his
6 tactical decisions.

7 And you heard from Captain Fulton that Pfc.
8 Manning was a good analyst and accomplished his
9 assigned tasks, which included pulling information
10 based on his knowledge of what the officer, she wanted
11 or needed about the enemy.

12 You also heard from Mr. Hall, a defense
13 expert qualified in the field of intelligence analyst,
14 even junior analyst, like Pfc. Manning, knew that the
15 enemy's capability and the enemy is just as capable as
16 piecing together information as our own junior analysts
17 are.

18 Although junior analysts are not expected
19 to that in-depth predictive analysis, they understand
20 the enemy's capabilities to use that information.

21 Your Honor, you also heard from Mr. Hall

1 that all analysts understand PIR, priority information
2 requirements. The gaps in intelligence information
3 that a commander has about the enemy, and how
4 intelligence analysts know this and work to answer
5 those specific gaps.

6 Your Honor, Pfc. Manning was a trained
7 analyst who understood how to assess the enemy and how
8 the enemy assesses U.S. Forces deployed.

9 Although not a senior analyst, Pfc. Manning
10 pulled data and conducted analysis to assist the senior
11 analysts with making actionable conclusions. He was
12 specifically trained on how the enemy also conducted
13 its own analysis and their capabilities to use
14 information about U.S. forces and the United States
15 national security and then fight against the United
16 States.

17 Your Honor, Pfc. Manning's knowledge of and
18 relationship with WikiLeaks, including when that
19 relationship began, is readily apparent when all the
20 evidence is considered together.

21 What is obvious is that Pfc. Manning pulled

1 as much information as possible to please Julian
2 Assange in order to get that information released and
3 Julian Assange found the right insider to mind SIPRnet
4 and the NIPRnet databases.

5 Pfc. Manning began data mining of SIPRnet
6 for intelligence relating to WikiLeaks organization
7 soon after arriving in theater. Or more precisely,
8 Your Honor, using his own words, right after
9 Thanksgiving timeframe of 2009. Those Lamo chats, Page
10 9.

11 Your Honor, Prosecution Exhibit 24.
12 Mr. Johnson found the, forensically found a file
13 containing the contact information for Julian Assange
14 and WikiLeaks, the leader of WikiLeaks, on Pfc.
15 Manning's external hard drive. This is the contact
16 information, Your Honor.

17 According to Mr. Johnson that file was
18 created on 29 November '09. 29 November '09. That is
19 less than two weeks after having access to SIPRnet that
20 Pfc. Manning then began using his SIPRnet access to
21 search Intelink for WikiLeaks.

1 We have heard testimony, Your Honor, that
2 3rd Brigade, 2nd Airborne finished the rip total with
3 210 Mountain in second week of November. Which means
4 by the beginning of December, that is the first two
5 weeks that Pfc. Manning had access to SIPRnet without
6 another soldier sitting to his left or right during the
7 (inaudible)

8 Your Honor, Special Agent Shaver testified
9 that Pfc. Manning searched Intelinks for the term
10 WikiLeaks more than 100 times beginning on 1
11 December 2009. Pfc. Manning also searched for Iceland
12 related topics 25 times between January and April 2010.
13 And also searched for Julian Assange in the same
14 timeframe.

15 You can see all the searches for WikiLeaks
16 on Prosecution Exhibit 81. Prosecution Exhibit 81,
17 Your Honor, is the summary of searches conducted by Pfc.
18 Manning from his SIPRnet computer.

19 And according to Prosecution Exhibit 81, he
20 conducted four searches for the term WikiLeaks, Your
21 Honor, for approximately every five days that he was at

1 FOB Hammer. Four searches for the term WikiLeaks every
2 five days, when he was at FOB Hammer.

3 Your Honor, one day after returning from
4 R&R leave Private First Class Manning compromised
5 (inaudible) and other Department of State information.
6 WikiLeaks published the cable a day later. In response
7 to the public release of that cable by WikiLeaks,
8 Private First Class Manning observed that the United
9 States Ambassador to Iceland was recalled or, as he put
10 it coldly, fired. That is in the Julian Assange chat,
11 Your Honor.

12 Your Honor, why would Pfc. Manning be
13 searching for and so focused on Iceland as an United
14 States Army analyst focused on Southeast Baghdad,
15 deployed in Iraq. Iceland searches relate back to
16 Julian Assange, who was in Iceland in February 2010 and
17 working on Islandic Modern Media Initiative.

18 Pfc. Manning knew that WikiLeaks would be
19 interested in matters pertaining to Iceland. That
20 could guarantee him real time disclosures actually on
21 the web, as fast as possible, for the world to access.

1 Your Honor, you heard evidence that Pfc.
2 Manning used other sources on the SIPRnet to gather
3 information on WikiLeaks as well. Just five days after
4 returning from R&R leave Pfc. Manning created an Open
5 Source Center account on 20 February 2010. And he used
6 the same moniker, BradS87, that he used in his Lamo
7 chats. Prosecution Exhibit 139 showed this
8 information.

9 Shaver testified that the same day Pfc.
10 Manning began using is OSC account to search for terms
11 like WikiLeaks in Iceland. Mr. Allen testified that
12 the Open Source Center with a website (inaudible)
13 Central Intelligence Agency containing reports,
14 translation and other information on unclassified
15 publications worldwide.

16 But it is not just a website providing news
17 updates. Special Agent Shaver testified that Pfc.
18 Manning searched for WikiLeaks at OSC more than 20
19 times. And information on Iceland more than 25 times.
20 Your Honor, why else would Pfc. Manning actively seek a
21 new account on the Open Source Center.

1 Julian Assange and Pfc. Manning discussed
2 the Open Source Center what is available. Julian
3 Assange stated that the OSC is, something we want to
4 mine entirely. That is the Julian Assange chats, Page
5 5.

6 WikiLeaks' interest in the Open Source
7 Center and Government analysis is also confirmed by
8 Most Wanted List, Prosecution Exhibit 109. Both
9 databases.

10 Defense corresponding exhibit. So what did
11 Pfc. Manning learn about WikiLeaks through all these
12 constant searches? The United States Government,
13 specifically United States Military, created three
14 classified U.S. Government reports that focused on the
15 threat WikiLeaks poses to the national security of the
16 United States; ACIC report, NCIS IRR and the C3
17 document.

18 First, Your Honor, the Army
19 counter-intelligence report on WikiLeaks. Between the
20 ACIC website logs at Prosecution Exhibit 63 and summary
21 of the ACIC document, Special Agent Shaver, Prosecution

1 Exhibit 84, Pfc. Manning viewed the ACIC report on at
2 least five separate occasions starting from less than
3 two weeks after access on SIPRnet on 1 December '09
4 through 7 March 2010.

5 ACIC report is Prosecution Exhibit 45 and
6 46. (inaudible) testified the purpose of the ACIC
7 document was to assess counter-intelligence threat to
8 the U.S. Army posed by WikiLeaks.

9 As you look at Prosecution Exhibit 45, Your
10 Honor, please note, note that the first bullet point
11 under key judgment of ACIC report is that WikiLeaks
12 represents a potential force protection,
13 counter-intelligence OPSEC and (inaudible) to United
14 States Army. Essentially the same language Pfc. Manning
15 used when he taught the dangers of OPSEC violations.

16 The second bullet states, recent
17 unauthorized releases of DoD sensitive and classified
18 information documents provide foreign intelligence
19 services, foreign terrorists groups, insurgents and
20 other foreign adversaries potentially actionable
21 information targeting U.S. forces.

1 Your Honor, the sixth bullet states that
2 WikiLeaks most likely has other DoD sensitive and
3 classified information in its possession and will
4 continue to post the information on the website.

5 Finally, the report concluded that it must
6 be presumed that foreign adversaries will review and
7 assess any DoD sensitive or classified information
8 posted for the WikiLeaks website.

9 Pfc. Manning sent reports to WikiLeaks with
10 the intent that they be released to the world. And it
11 was, Your Honor.

12 Your Honor, second, the intelligence
13 information IRR, dated 23 March 2008 titled Internet
14 Web Posting of classified and official use only
15 documents. Prosecution Exhibit 99.

16 First, Your Honor, what is IRR? That's a
17 report used by intelligence professionals to report
18 analysis of raw intelligence. The purpose of this IRR
19 was to raise the awareness as a threat to national
20 security.

21 Special Agent Shaver that he created

1 Prosecution Exhibit 85. That was a summary of the
2 intel log information related to the IRR, and later I
3 will talk about, Your Honor, a C3 document.

4 THE COURT: What exhibit?

5 MAJOR FEIN: Exhibit 85. That summary
6 relates to and shows that Pfc. Manning downloaded this
7 report on 14 February 2010. Found on Line 19 of that
8 exhibit.

9 The purpose of that IRR was to raise the
10 awareness of the threat caused by WikiLeaks to the
11 intelligence community. IRR discussed WikiLeaks is
12 publicly accessible website where the leaked
13 information includes classified and for official use
14 only, can be published to the public anonymously.

15 The report described the threat of
16 publishing classified information. It also detailed
17 the release of a Camp Delta SOP, GITMO, that was
18 unclassified, for official use only and caused concerns
19 within the United States Government.

20 Your Honor, Pfc. Manning also compromised
21 this document to WikiLeaks. Line 5 of Prosecution

1 Exhibit 127. That's a volumes.txt data. That is when
2 a CD was burned on a SIPRnet computer, date and time of
3 that burn, the file name and folder structure. And
4 that was created on his personal Mac. Once you take a
5 CD, burn, put it into the Mac computer it creates a log
6 file.

7 That was Line 5, Your Honor. Third, the
8 report dated 7 January 2010, that I have already
9 referenced is a 3C report. This is the trip report
10 discussing the Marine Corp monitoring the chaos
11 communications Congress that was held 26 to 30 December
12 2009 in Germany.

13 This report, Your Honor, Prosecution
14 Exhibit 43. Your Honor, going back to Prosecution
15 Exhibit 85, the summary that Special Agent Shaver
16 created for the IRR, the 3C document. Line 12 shows
17 that Pfc. Manning downloaded that document 14 February
18 2010 as well.

19 (Inaudible) the author of the document
20 testified that the document was posted to its unit
21 portal on SIPRnet and the address at Line 12 was the

1 address for that article.

2 Sergeant (inaudible) also testified that
3 the purpose of the report was to identify a potential
4 threat by WikiLeaks, particularly a security threat
5 that the owners may be vulnerable to. And then his
6 analysis was how to fix that vulnerability. The report
7 discussed that WikiLeaks publicly accessible internet
8 website, leaked information, including classified
9 information can be published.

10 On Page 3 of Prosecution Exhibit 43, the
11 report, analysis states, WikiLeaks.org poses a large
12 threat not only from the external disclosure but also
13 from the insider. The insider within the Department of
14 Defense. The insider would be able to leak information
15 without fear of any direct individual repercussions.

16 Your Honor, Pfc. Manning compromised this
17 document to WikiLeaks. That is clear by looking at the
18 file titled C3 on the .txt printout, Prosecution
19 Exhibit 127.

20 Your Honor, through his constant searches,
21 systematic review of intelligence reports, Pfc. Manning

1 knew exactly what type of information he was providing
2 classified information to an organization that diverse
3 elements of the U.S. Military reported was a threat to
4 the national security interest of United States
5 Government.

6 Your Honor, in addition to the research
7 that he conducted, also looked at Pfc. Manning's actual
8 thoughts on WikiLeaks, as captured in his chat logs
9 with Lamo and Julian Assange.

10 These chat logs confirm that Pfc. Manning
11 saw WikiLeaks as anything but a journalistic
12 enterprise. Pfc. Manning saw WikiLeaks as an
13 intelligence agency. And that Pfc. Manning knew that
14 WikiLeaks' goals in the methods were different than
15 anything that could be characterized as traditional
16 journalism.

17 Your Honor only needs to look as far as the
18 chats to Julian Assange, Prosecution Exhibit 123. That
19 is the Assange chats. Page 9, Your Honor. Pfc. Manning
20 identified WikiLeaks as the first intelligence agency
21 for the general public. And in his own words, because

1 it did everything an intelligence agency does, minus
2 the anonymous sourcing.

3 Page 10 of the chats, Your Honor, Julian
4 Assange confirmed this evaluation and noted that the
5 original WikiLeaks described WikiLeaks as the first
6 intelligence agency of the people, better principled
7 and less parochial than any Government intelligence
8 agency. Its only interest in revelation of the truth.

9 Even when discussing the substantive of the
10 information that he compromised Pfc. Manning
11 acknowledged what was in the documents would make it
12 look more like a journalist acquired it. That's on
13 Page 2.

14 And what did Julian Assange say about his
15 operation to Pfc. Manning? He talked about giving an
16 Intel source a list of things he wanted. Page 7. He
17 talked about outing another spy this afternoon. Page
18 11.

19 He asked Pfc. Manning if there's some way I
20 can get you a crypto phone? Page 11. Crypto phone,
21 secure communications with Pfc. Manning in Southeast

1 Baghdad.

2 Pfc. Manning knew anything he disclosed
3 WikiLeaks would be published on the internet for the
4 world to see. It is clear Pfc. Manning wanted this
5 information to be in the public domain.

6 The ACIC report, which Pfc. Manning
7 repeatedly read and compromised, discusses the DoD
8 classified information that WikiLeaks released in the
9 past and how WikiLeaks posts all information they
10 receive without editorial oversight.

11 The ACIC report also says that WikiLeaks
12 aimed for maximum political impact. The C3 document
13 stated that the goal of WikiLeaks was to create
14 openness. And Prosecution Exhibit 30, these are the
15 chats, Lamo chats, Your Honor, Pfc. Manning admitted
16 that he transferred his documents to WikiLeaks, he
17 couldn't let these things stay inside the system and
18 inside of his head. Page 26.

19 He also specifically admitted that the
20 information he sent to WikiLeaks belongs to the board
21 of public domain, the information should be free. Page

1 40. He also stated about the Apache video. Event
2 occurring 2007, I watched video in 2009 with no context
3 to research, forward information to a group of Freedom
4 of Information Act. Page 33.

5 Your Honor, the chats with Assange. Pfc.
6 Manning says, I told you before Government
7 organizations can't control information. The harder
8 they try the more violently the information wants to
9 get out. That's Page 5, Your Honor.

10 When discussing WikiLeaks obtaining
11 information from a public figure's email account and
12 posting that information, Pfc. Manning says, well, I
13 don't know what a posting of a list of (inaudible) but,
14 hey, its transparency. Page 5.

15 Your Honor, setting aside semi-classified
16 documents to established journalistic enterprise like
17 New York Times or Washington Post would be a crime.
18 That is not what happened in this case under these
19 facts.

20 Pfc. Manning deliberately and intentionally
21 disclosed his compromised information through WikiLeaks

1 to the world knowing that WikiLeaks would release the
2 information in the form they received it and that is,
3 Your Honor, that is exactly what happened in this case.

4 WikiLeaks was merely the platform which Pfc.
5 Manning used to ensure all the information was
6 available for the world, including the enemies of the
7 United States.

8 Your Honor, Defense offered Professor
9 Benkler as an expert in the network for (inaudible).
10 Professor Benkler's opinion is based on bias,
11 misinformation and a flawed methodology. It provides
12 no utilities because regardless of his conclusions,
13 Your Honor, Professor Benkler can give you no insight
14 in what Pfc. Manning was thinking at the time he was
15 deployed.

16 Professor Benkler based his opinions
17 largely on a review of articles, news articles, post
18 July 2010, several months after Pfc. Manning was placed
19 in pretrial confinement.

20 However, if there's any utility to
21 Professor Benkler's testimony it was in his answers to

1 several questions posed to him on journalistic
2 enterprises, in general, questions that used Pfc.
3 Manning's own words.

4 Professor Benkler agreed that a
5 transparency movement is not a journalistic enterprise.
6 He agreed that information activist is not a
7 journalistic enterprise. He agreed there's a
8 difference between activism and journalism.

9 WikiLeaks, an organization with a mission
10 for transparency of U.S. Government classified
11 information for the purpose of maximizing political
12 impact. Information -- well, essentially, Your, Honor
13 information anarchist. That failed to meet even
14 Professor Benkler's criteria for a journalistic
15 enterprise.

16 Your Honor, Professor Benkler testified
17 that his main sources of information were the news
18 articles he reviewed, which he then assigned values to
19 in some way that's not entirely transparent. And used
20 some critiques he received from Julian Assange when he
21 posted his draft article on his personal web page.

1 Professor Benkler conducted no independent
2 research on any aspect of WikiLeaks, including the ACIC
3 reports, or WikiLeaks, nor did he interview anyone with
4 firsthand knowledge of WikiLeaks.

5 He clearly had a point of view and strong
6 opinions. But Professor Benkler did not have access to
7 the evidence in this case revealing what Pfc. Manning
8 actually knew and thought of the WikiLeaks
9 organization, nor did he have access to the evidence
10 that demonstrated how WikiLeaks actually operated
11 outside the news report he analyzed and researched.

12 Reporting that any knowledge was very poor
13 at the time. As an example of professor Benkler's
14 faulty process, he concluded that WikiLeaks acted
15 responsibly by characteristic of a traditional news
16 media, hand selected or redacted December cables in
17 2010.

18 He spent much time testifying that
19 80 percent incorrectly reported that WikiLeaks released
20 over 250,000 Department of State cables onto the
21 internet at that time, when he counted only 272 cables

1 based on other news reports, correlating news reports.

2 He further concluded that WikiLeaks
3 continued to follow that model in all of their
4 releases. Had Professor Benkler actually conducted
5 independent research outside of news reports, such as
6 contacting WikiLeaks, editors of newspapers, or any
7 other person with firsthand knowledge, he would have
8 quickly realized that WikiLeaks actually did release
9 251,287 purported cables on the internet in unredacted
10 form, as well as other databases of information that
11 Pfc. Manning compromised.

12 Your Honor, regardless of what Professor
13 Benkler, the Defense of United States believes
14 WikiLeaks is or is not, the evidence is clear that Pfc.
15 Manning believed the organization to be his conduit to
16 release as much information as he could obtain.

17 But why did he choose WikiLeaks? He chose
18 WikiLeaks because they sought, almost exclusively, from
19 the United States, United States Government classified
20 information, and that is what Pfc. Manning could provide
21 them as an intelligence analyst on SIPRnet.

1 The three intelligence reports, all said
2 that WikiLeaks, any type of classified information as
3 well as PII and their operational data. In chats with
4 Julian Assange Pfc. Manning showed his understanding
5 that WikiLeaks was seeking to publish Government
6 controlled information, said to them by him and other
7 donors.

8 Your Honor, that shows that WikiLeaks
9 produced a Most Wanted List available on its website.
10 That it identified to the reader the type of
11 information that they sought, to gather and disclose in
12 the name of transparency information anarchy. Looking
13 at both versions of the Most Wanted List, Prosecution
14 Exhibit 109 or 110 and the Defense unsorted list,
15 Defense Exhibit Foxtrot or Defense Exhibit Papa.

16 The largest section on the Most Wanted List
17 by several orders of magnitude, Your Honor, was the
18 section devoted to the United States, specifically the
19 section devoted to military intelligence documents on
20 Prosecution Exhibits 109 and 10 in bulk databases on
21 Defense Exhibits Foxtrot and Papa.

1 Less than two weeks after Pfc. Manning had
2 regular access to SIPRnet, Pfc. Manning began using
3 Intelink to search for items on that Most Wanted List.
4 (Inaudible) Prosecution Exhibit 81, you'll see the
5 searches on 28 November, 29, 30 November and 8 December
6 '09, that correspond with items on the Most Wanted
7 List. None of these have any relationship to a United
8 States Army Intelligence Analyst assigned to Southeast
9 Baghdad focused on a (inaudible)

10 Specifically, Your Honor, by 28
11 November 2009, Thanksgiving, Pfc. Manning was searching
12 for information related to GITMO and interrogations.
13 Prosecution Exhibit 81 is a summary of those.

14 The Most Wanted List in 2009 shows that
15 WikiLeaks wanted CIA interrogation videos. Pfc. Manning
16 searched for retention of interrogation videos. The
17 term retention of interrogation videos on 28 and 29
18 November 2009. That is Line 28 through 32 of PE 81.

19 Pfc. Manning continued searching for
20 detainee videos on 9 December. Retention of
21 interrogation videos on Lines 28 through 32 of PE81.

1 Your Honor, Pfc. Manning continued searching
2 for detainee videos on 9 December. That's Line 115
3 through 116. He conducted more searches for
4 interrogation videos on 17 December. Line 154 through
5 155. He conducted another search a month later at
6 Line 283.

7 Your Honor, the Most Wanted List of 2009
8 also shows that WikiLeaks wanted detainee abuse photos.
9 Their term. Pfc. Manning searched for the term detainee
10 abuse on 29 and 30 November, 2009. Lines 44 through
11 46. Line 63.

12 The Most Wanted List showed that WikiLeaks
13 wanted Camp Delta, Guantanamo standard operating
14 procedures. And Camp Delta, Guantanamo interrogation
15 standard operating procedures, 2003 through 2009.

16 Your Honor, Pfc. Manning searched for
17 Guantanamo detainee operations, JTF, GITMO SOP and SOP
18 interrogation, among others, on 8 December. This is at
19 Line 101 through 112.

20 Pfc. Manning continued the search throughout
21 his deployment. 15 March Pfc. Manning searched Intelink

1 for information on GITMO, ISN and search. That was on
2 Line 470 through 474.

3 Your Honor, Pfc. Manning spent hours, hours
4 in late November 2009, early in December 2009,
5 searching for topics that only related to one mission,
6 finding and disclosing what WikiLeaks wanted.

7 He was not a naive soldier simply affected
8 by an event on 24 December 2009, an event that only
9 Chief Ehresman vaguely remembers, not even the exact
10 date, but rather Pfc. Manning was deliberately taking
11 advantage of the trust and access to classified systems
12 in pursuit of his own objectives.

13 Think back to one of the first things that
14 Pfc. Manning said to Lamo in the chats. If you had
15 unprecedented access to classified networks, what would
16 you do?

17 Pfc. Manning answered that question with his
18 actions. He searched for as much information that he
19 knew would guarantee his fame, information that
20 WikiLeaks wanted to publicly release.

21 Your Honor, although he kept searching for

1 information on WikiLeaks' Most Wanted List, Pfc. Manning
2 also wanted to ensure he would not get caught.

3 So why did Pfc. Manning chose to disclose
4 classified information through WikiLeaks and not solely
5 by himself for the world to have? He did not want to
6 get caught, Your Honor. Pfc. Manning anticipated
7 needing to slip into the darkness for a few years, let
8 the heat die down. At least that's what he said to
9 Julian Assange on the chats on Page 5.

10 Prosecution Exhibit 42. He instructed
11 WikiLeaks to protect their source, protect him. The
12 ACIC report on the IRR, informed Pfc. Manning as early
13 as December '09, that WikiLeaks used anonymous methods
14 to post information online.

15 The ACIC report detailed that WikiLeaks
16 uses its own software which can make it difficult for
17 foreign governments and foreign business to determine
18 where the leak document was and who is responsible for
19 leaking that document.

20 Your Honor, the IRR described WikiLeaks as
21 an uncensorable Wikipedia for untraceable mass document

1 leaking analysis. The IRR concluded that the WikiLeaks
2 website provides suggestions for the anonymous
3 submission of material and several methods of
4 submitting material for inclusion to an online
5 database.

6 Your Honor, right now might be a good time
7 for a brief recess before I get going.

8 THE COURT: All right. How much longer do
9 you anticipate your argument is going to be? I'm
10 looking at whether we should recess for lunch.

11 MAJOR FEIN: I can probably get through one
12 more section and then recess for lunch. Overall, I
13 anticipate two more full hours.

14 THE COURT: Why don't we take a 15-minute
15 recess, get through the next session and take a lunch
16 break.

17 MR. COOMBS: I would like to know maybe how
18 long the section is. If the next session is an hour, I
19 would rather break for lunch now.

20 MAJOR FEIN: It's not. Actually, I can
21 probably get to the next session, right now it is the

1 first set of data that was compromised. Probably last
2 15 minutes. The section after that is lengthy, Your
3 Honor, after the next section.

4 THE COURT: All right. Mr. Coombs, do you
5 have any grave objection here to taking a quick
6 15-minute recess, finishing up with that 15 minutes and
7 then taking a lunch break after that?

8 MR. COOMBS: No, objection, Your Honor.

9 THE COURT: The Court will recess until
10 five after 12:00.

11 (Recess)

12 THE COURT: Court is called to order.
13 Record show that all parties present when the Court
14 last recessed are present in Court. Major Fein.

15 MAJOR FEIN: Yes, ma'am. The first dataset
16 is (inaudible). This case starts with Pfc. Manning's
17 admission to Mr. Lamo that he had helped WikiLeaks
18 right at Thanksgiving 2000.

19 How did Pfc. Manning begin helping
20 WikiLeaks? By transmitting the video file charged in
21 Specification 11, Charge 2.

1 Specification 11 in Charge 2. Your Honor,
2 what we know about the Granai airstrike video and why
3 is it important? Pfc. Manning admitted to Adrian Lamo
4 that he gave it to WikiLeaks. Lamo chat logs, Page 46.
5 Jason Katz, an employee of Brookhaven National labs had
6 a copy on his computer dated 15 December 2009.

7 We know that the video was encrypted
8 (inaudible). We know that WikiLeaks tweeted on 8
9 January 2010, that they needed assistance with
10 decrypting a video. These are undisputed facts.

11 So why, Your Honor, is the Defense fighting
12 so hard to disprove this timing? Because the evidence
13 destroys, Your Honor, their narrative that Pfc. Manning
14 witnessed an event that helps explain his actions
15 rather than accepting the facts as they -- Pfc. Manning
16 was only interested in disclosing classified
17 information to the world through WikiLeaks.

18 We start within weeks of having access to
19 SIPRnet. And he chose a video that he could not even
20 watch, a password protected video.

21 Pfc. Manning accessed this video before 1

1 December 2009 (inaudible). He transferred the video to
2 his personal Mac and uploaded to WikiLeaks before 15
3 December 2009. So that lands in the hands of a person
4 willing to assist WikiLeaks with a mass decryption
5 effort.

6 THE COURT: Can you speak a little more
7 slowly?

8 MAJOR FEIN: Yes, Ma'am. Pfc. Manning
9 accessed this video before 1 December 2009. That was
10 on the (inaudible) server. He transferred the video to
11 his personal Mac and uploaded it to WikiLeaks before 15
12 December 2009.

13 He did that, Your Honor, so it could land
14 in the hands, to assist in the decryption effort.

15 Your Honor, how do we know this? Special
16 Agent Shaver testified that BE22PAX.zip, that file name
17 contained in the video file within zip file called
18 BE22PAX.wmv. WMV is the Windows file, Windows movie
19 video type.

20 That video was located in the U.S.
21 (inaudible) site with documents that were part of the

1 (inaudible) investigation.

2 According to multiple U.S. CentCom subject
3 matter experts the investigation was focused on
4 investigating the circumstances surrounding a civilian
5 casualty (inaudible) incident.

6 Your Honor, Prosecution Exhibit 65 did the
7 (inaudible). In that exhibit, you'll see the file
8 BE22PAX.zip, which is also listed on the charge sheet,
9 is under the folder called videos.

10 Multiple CentCom witnesses testified video
11 operational activities, including troop movement,
12 weapon systems and specific information contained on
13 the heads up display.

14 In classified testimony, through a
15 stipulation of expected testimony that the video
16 reveals other details of military preparedness.

17 Your Honor, what we know forensically about
18 Pfc. Manning in the late November 2009 and early
19 December 2009 time period, Your Honor, between 29
20 November 2009 and 9 December 2009, Pfc. Manning searched
21 several times on SIPRnet intelling specifically for the

1 terms SJA and CentCom. That's in Prosecution Exhibit
2 81.

3 Those searches would have brought Private
4 First Class Manning to the U.S. SJA website, the legal
5 website, Intel only shows searches and redirects, as
6 you heard Special Agent Shaver, to other websites.
7 They don't actually account for activity. It's on a
8 separate server. The CentCom SharePoint server was a
9 separate server.

10 Mr. Moser, senior paralegal for the U.S.
11 CentCom SJA office and the administrator of the U.S.
12 SharePoint page, he testified the (inaudible) videos
13 located on SharePoint server.

14 Your Honor Prosecution Exhibit 91 is a copy
15 of the portal web page. Five screen shots of that
16 page, Your Honor. Note, Your Honor, when you review
17 Prosecution Exhibit 91, across the top each of the web
18 pages is a red banner. And that red banner has
19 "secret" approximately five times spread across the top
20 of that page.

21 Prosecution Exhibit 91 screen shots all the

1 different folders within the SJA investigations share
2 the (inaudible) that leads to videos BE22PAX.zip. Your
3 Honor, that banner put any visitor, including Pfc.
4 Manning, on notice that the information on that website
5 should at least be treated classified.

6 Special Agent Shaver (inaudible) duplicate,
7 Your Honor, of that on Jason Katz's computer. Although
8 the file he found was named B.zip. Jason Katz, an
9 employer of the laboratory created B.zip on 15
10 December 2009. Had his computer plug into the lab's
11 super computer, which is capable of breaking into or
12 decrypting files.

13 Your Honor, Prosecution Exhibit 32 is a
14 tweet from WikiLeaks on 8 January 2010, which states,
15 having crypt-ed videos of U.S. bomb strikes on
16 civilians with a web page, says Afghan, we need super
17 computer time. That was on 8 January 2010.

18 Your Honor, this WikiLeaks tweet, the
19 encrypted file on Katz's computer, which is connected
20 to the super computer, and Pfc. Manning's admissions,
21 all lead to one conclusion. The transmission of the

1 video occurred prior to 15 December 2009. And based on
2 the evidence available to the Court, there's no other
3 reasonable explanation.

4 And here's why, Your Honor. First Special
5 Agent Shaver, Mr. Johnson, the other forensic examiner,
6 testified they did not find any remnants or evidence of
7 the videos running videos on any of the computers they
8 examined.

9 We know that nothing was recoverable by the
10 personal act before the 31 January 2010 or SIPRnet
11 computers from March 2010, because they were reimaged.
12 Personal Mac, because he forensically wiped his
13 computer using a 7 pass forensic wipe. Pfc. Manning did
14 that.

15 Second, Your Honor, Special Agent Shaver
16 testified that when he reviewed the U.S. CentCom
17 SharePoint server logs, so the actual server logs that
18 housed the videos, that's Prosecution Exhibit 108. The
19 log started on 1 December 2009. They captured all the
20 access activity of the files in the folder that sat on
21 the CentCom website.

1 Those logs, Your Honor, 1 December 2009.

2 After that date the logs showed that the video was only
3 accessed twice. Once on 28 January 2010 and again on
4 23 February 2010.

5 Now first, Your Honor, Pfc. Manning could
6 not have accessed the video on that date because he was
7 in Boston on R&R leave. Pfc. Manning did not access the
8 video on 23 February 2010. The reason we know that is
9 because of the Centaur logs. That captured threat data
10 for this case between Pfc. Manning's SIPRnet computers
11 and other destinations do not show any connections to
12 the CentCom SharePoint server on 23 February 2010.

13 Now, Your Honor, note at Prosecution
14 Exhibit 161, Special Agent Shaver testified that he
15 created this summary, Prosecution Exhibit 161, that
16 shows all the missing dates from the Centaur logs. So
17 his testimony was, the Centaur logs were complete, but
18 he testified that certain days he knew were complete
19 because there were some activity that showed and other
20 days it was completely void.

21 At line 58 of Prosecution Exhibit 161

1 showed that 23 February 2010, was reported within
2 Centaur and not missing from the logs. And there was
3 no entry from the a logs, as Special Agent Shaver
4 testified, between Pfc. Manning's SIPRnet computer and
5 the portal on 23 February 2010.

6 Third, at trial the Defense referenced the
7 video file titled (inaudible). You heard testimony
8 that it was located in a folder named (inaudible), a
9 shared drive at FOB Hammer.

10 This file, Your Honor, on a Microsoft
11 Windows computer, keeps track of the last ten times a
12 file type is opened. WMV.

13 Special Agent Shaver testified that
14 (inaudible) was listed in the NT user file under the
15 WMV file type on Pfc. Manning's SIPRnet computer. Your
16 Honor, this means that Pfc. Manning opened (inaudible)
17 on his SIPRnet computer.

18 The issue here is that it could not be
19 BEPAX22.WMV because that video, the charge video was an
20 encrypted zip file. Thus, unable to be opened and
21 viewed by Pfc. Manning. And could not show up in the NT

1 user file as a WMV viewed file.

2 Your Honor, fourth, Prosecution Exhibit 128
3 is the summary of all the (inaudible) related activity
4 in the index.dac file on Pfc. Manning's SIPRnet
5 computer. That's Prosecution Exhibit 128.

6 Special Agent Shaver testified in the
7 index.dac records, that file records the dates and
8 times the files are accessed either locally or remotely
9 through a web browser for Windows.

10 Also testified on 10 April 2010, the day
11 Pfc. Manning downloaded the entire investigation, less
12 the videos, from the SharePoint site, there was no
13 video file or zip file reflected in the activity on his
14 SIPRnet computer. All the other files were downloaded
15 but not a zip file or WMV file.

16 Your Honor, look at Prosecution Exhibit
17 129. That is the summary of the logs on 10 April 2010.
18 Index.dac, Prosecution Exhibit 128, shows activity Pfc.
19 Manning's computer connecting to SharePoint logs and
20 Exhibit 129 next in line, a summary of the actual
21 SharePoint logs from the CentCom website. Activity on

1 10 April 2010.

2 The CentCom logs show the other side of the
3 download transaction. The CentCom site. Every
4 document downloaded from the CentCom SharePoint site on
5 10 April 10 that is associated with Farah is located in
6 that summary.

7 Most importantly, Your Honor, there is no
8 video CentCom downloaded during that time on those logs
9 also.

10 Your Honor, the video must have been
11 downloaded prior to 1 December 2009 and transmitted no
12 later than 15 December 2009. Your Honor, Pfc. Manning
13 knew his video along with the other videos were
14 classified.

15 Although the file name did not have
16 annotation, the file was located on SIPRnet with a
17 secret banner across the top of his scene. The video
18 relates to the national defense of the United States,
19 which the video contained the type of information which
20 could cause serious harm to national security and thus
21 should be secret.

1 (Inaudible) U.S. CentCom Deputy Commander
2 duly appointed original classification authority
3 testified that the charge video was properly classified
4 at the secret level. And, Your Honor, the United
5 States Government has never made this video available
6 to the public as part of a 15-6 or any other.

7 Now at this time would be a good time for
8 lunch recess.

9 THE COURT: All right. We can come back at
10 1330. Does that work for everybody?

11 MR. COOMBS: Yes, ma'am.

12 THE COURT: Court is in recess until 1330.

13 (Recess at 1:30 p.m.)
14
15
16
17
18
19
20
21

A	acted (1) 62:14	affected (1) 67:7	among (2) 39:20;66:18
	action (2) 9:20;27:15	Afghan (1) 75:16	amount (2) 28:3;42:15
abide (1) 24:6	actionable (2) 45:11;51:20	Afghanistan (1) 15:17	amounts (2) 11:16;16:13
ability (2) 5:19;14:21	actions (3) 41:3;67:18;71:14	afternoon (1) 57:17	analyses (1) 30:13
able (2) 38:5;55:14	actively (1) 49:20	again (8) 4:5;5:14;6:10,21;7:20; 32:10,12;77:3	analysis (22) 31:21;40:15,16;42:7; 43:8,9,10,12,14,15,18; 44:4,5,19;45:10,13;50:7; 52:18;55:6,11;69:1
absent (2) 4:6,19	activism (1) 61:8	against (6) 22:3,3;23:2;33:3;43:2; 45:15	analyst (25) 8:12;12:8;17:12,14;21:7; 24:20;30:2;31:1;36:8,14; 37:21;38:8,14;39:1,6;43:5, 21;44:8,13,14;45:7,9;48:14; 63:21;65:8
abuse (2) 66:8,10	activist (1) 61:6	agency (8) 11:4,6;49:13;56:13,20; 57:1,6,8	analysts (20) 30:13;32:5;37:21;38:15, 17,20;39:11,14,15;40:1,6,8, 12,21;41:19;44:16,18;45:1, 4,11
abused (2) 8:13;27:20	activists (1) 35:11	Agent (15) 20:3;47:8;49:17;50:21; 52:21;54:15;72:16;74:6; 75:6;76:5,15;77:14;78:3, 13;79:6	analyze (2) 41:6,8
Abusing (1) 10:4	activities (4) 20:17;21:1;30:5;73:11	agreed (3) 61:4,6,7	analyzed (1) 62:11
accepted (2) 26:17,18	Activity (15) 9:14;16:6,13;39:16; 41:16;42:13;43:13,13;74:7; 76:20;77:19;79:3,13,18,21	agreement (4) 25:7;26:18;27:2,6	anarchist (1) 61:13
accepting (1) 71:15	acts (2) 10:14;33:7	agreements (5) 25:9,20;27:12,14,17	anarchy (2) 9:6;64:12
access (26) 10:4,15;11:13;16:9,20; 17:12;21:18;25:3,11;27:3, 19,20;36:20;46:19,20;47:5; 48:21;51:3;62:6,9;65:2; 67:11,15;71:18;76:20;77:7	actual (7) 12:13;18:5;29:15;32:21; 56:7;76:17;79:20	aided (1) 13:8	anguished (1) 9:18
accessed (6) 16:11;71:21;72:9;77:3,6; 79:8	actually (14) 6:13;7:8;9:2;10:11; 12:15;30:16;31:1;48:20; 62:8,10;63:4,8;69:20;74:7	aimed (1) 58:12	Anika (2) 31:11,17
accessible (4) 29:6;38:20;53:12;55:7	addition (3) 23:18;29:20;56:6	Airborne (1) 47:2	annotation (1) 80:16
accomplish (2) 17:13;40:20	additional (2) 5:1;29:13	airstrike (2) 15:21;71:2	anonymous (3) 57:2;68:13;69:2
accomplished (1) 44:8	Additionally (1) 4:7	AIT (9) 17:16,17,21;21:15;22:20; 24:21;28:1;29:20;32:16	anonymously (2) 11:15;53:14
accordance (1) 5:21	address (4) 7:11;16:19;54:21;55:1	allegiance (1) 8:4	answered (1) 67:17
according (6) 20:11;30:3;32:9;46:17; 47:19;73:2	addresses (1) 34:20	Allen (1) 49:11	anticipate (2) 69:9,13
account (6) 4:3;49:5,10,21;59:11; 74:7	administrator (1) 74:11	allowed (2) 18:16;19:10	anticipated (1) 68:6
accountable (2) 33:6,11	admission (1) 70:17	allows (2) 40:8;41:12	Anti-Terrorism (1) 28:18
accounting (1) 5:7	admissions (1) 75:20	almost (1) 63:18	Apache (3) 20:4,9;59:1
accrue (1) 8:9	admitted (5) 13:13;23:19;58:15,19; 71:3	along (2) 34:10;80:13	apparent (1) 45:19
ACIC (12) 50:16,20,21;51:1,5,6,11; 58:6,11;62:2;68:12,15	Adrian (2) 15:2;71:3	al-Qaida (7) 13:10,11;22:19;23:10,12; 29:18,19	Appellate (4) 5:2,9,11;6:2
acknowledged (1) 57:11	advanced (1) 6:14	alternate (1) 4:13	Appendix (1) 29:8
acknowledgments (2) 10:7;25:10	advantage (1) 67:11	Although (6) 13:18;44:18;45:9;67:21; 75:7;80:15	Apple (1) 14:12
acquired (1) 57:12	adversaries (6) 26:11;35:8,13;36:12; 51:20;52:6	Always (1) 21:3	applicable (1) 42:9
across (5) 16:6,15;74:17,19;80:17	adversary (1) 21:4	Ambassador (1) 48:9	appointed (1)
Act (2) 59:4;76:10	advise (1) 7:5		

81:2 appreciated (1) 12:9 approximately (3) 32:10;47:21;74:19 April (7) 16:14;26:4;47:12;79:10, 17:80:1,5 Arabian (2) 13:11;29:19 area (2) 31:21;32:8 areas (2) 30:6;43:19 argues (1) 14:3 argument (8) 5:13;6:15;7:6,7,8,12; 12:1;69:9 arise (1) 7:2 armed (3) 8:7,8;13:6 arms (2) 30:9;43:2 army (18) 15:12;18:6,14;26:5;28:2, 13,17;29:1,7;35:6;39:1; 41:2,11;48:14;50:18;51:8, 14;65:8 Army's (1) 34:11 arrived (2) 32:15,17 arriving (2) 8:13;46:7 art (1) 43:12 article (2) 55:1;61:21 articles (3) 60:17,17;61:18 aside (1) 59:15 aspect (1) 62:2 Assange (22) 11:3;14:16;15:2;17:3; 46:2,3,13;47:13;48:10,16; 50:1,3,4;56:9,18,19;57:4, 14;59:5;61:20;64:4;68:9 assess (3) 45:7;51:7;52:7 assesses (1) 45:8 assessment (2) 31:20;43:6 assessments (1) 31:21 assets (2) 34:6,6 assigned (8) 32:12;36:14;38:17;39:2;	40:13;44:9;61:18;65:8 assist (4) 17:3;45:10;72:4,14 assistance (2) 32:7;71:9 assisting (1) 11:12 associated (1) 80:5 assume (1) 21:3 assurance (2) 23:20;24:16 attack (2) 9:7;22:16 attacks (2) 30:7;42:16 attempt (1) 20:15 attended (1) 17:17 audience (1) 21:2 audit (1) 16:4 author (1) 54:19 authorities (2) 18:15;19:9 authority (1) 81:2 authorized (2) 21:11,12 available (8) 4:14;17:8;29:3;50:2; 60:6;64:9;76:2;81:5 avoid (1) 35:21 aware (1) 10:19 awareness (2) 52:19;53:10	40:10 battlefield (1) 34:11 BE22PAXwmv (1) 72:18 BE22PAXzip (3) 72:16;73:8;75:2 began (5) 45:19;46:5,20;49:10;65:2 begin (1) 70:19 beginning (2) 47:4,10 behavior (1) 43:12 believes (1) 63:13 belongs (1) 58:20 benefit (1) 44:1 benefits (1) 44:1 Benkler (9) 60:9,13,16;61:4,16;62:1, 6;63:4,13 Benkler's (4) 60:10,21;61:14;62:13 BEPAX22WMV (1) 78:19 best (2) 9:7;11:20 better (1) 57:6 bias (1) 60:10 bigger (1) 10:5 bin (1) 23:10 birth (1) 34:20 blackmail (1) 26:11 blog (1) 21:2 blue (1) 19:1 board (1) 58:20 bold (1) 20:21 bomb (1) 75:15 borne (1) 31:20 Boston (1) 77:7 both (5) 24:16;27:16;44:4;50:8; 64:13 bottom (2) 19:2;21:4	box (1) 4:10 Bradley (2) 8:3;34:1 BradS87 (1) 49:6 break (4) 7:14;69:16,19;70:7 breaking (1) 75:11 brief (6) 7:13,17;28:11;31:14; 42:18;69:7 briefed (2) 26:4,7 briefing (5) 15:13;18:3;19:19;34:13; 35:20 briefly (1) 6:18 brigade (5) 31:15;36:16;37:1;43:3; 47:2 bright (1) 20:21 Brookhaven (2) 15:20;71:5 brought (4) 15:6,11;33:5;74:3 browser (1) 79:9 Buchannon (1) 39:17 building (1) 36:16 bulk (1) 64:20 bullet (3) 51:10,16;52:1 burn (2) 54:3,5 burned (3) 15:5;20:8;54:2 business (1) 68:17 Bzip (2) 75:8,9
	B		C
	back (4) 48:15;54:14;67:13;81:9 background (1) 40:3 bad (1) 31:14 Baghdad (4) 40:17;48:14;58:1;65:9 Balonek (3) 27:8;30:16,18 banner (4) 74:18,18;75:3;80:17 based (9) 24:4;41:3;43:13;44:2,10; 60:10,16;63:1;76:1 basis (2) 37:15;42:19 battalion (1)		C3 (4) 50:16;53:3;55:18;58:12 cable (2) 48:6,7 cables (4) 62:16,20,21;63:9 calculating (1) 10:13 called (7) 4:2;7:18;21:5,18;70:12; 72:17;73:9 came (2) 6:19;32:5

Camp (3) 53:17;66:13,14	15:1,5;32:8;40:3;41:16; 77:18	11,14;26:5,12;27:3,7,13,19, 21;33:8;36:17;37:5,9,14,16; 38:1;50:14;51:17;52:3,7, 14;53:13,16;55:8;56:2; 58:8;61:10;63:19;64:2; 67:11,15;68:4;71:16;73:14; 75:5;80:14;81:3	complete (3) 39:2;77:17,18
can (18) 5:21;18:10;21:19;22:16; 23:2;24:12;25:20;41:8; 47:15;53:14;55:9;57:20; 60:13;68:16;69:11,20;72:6; 81:9	certificates (1) 23:20		completed (1) 23:21
capabilities (7) 23:6;29:3;34:11;35:5; 39:9;44:20;45:13	changed (1) 4:19		completely (1) 77:20
capability (1) 44:15	chaos (1) 54:10	classify (1) 18:15	complexity (1) 11:20
capable (3) 29:9;44:15;75:11	chapel (1) 4:14	classifying (1) 18:13	complied (1) 39:10
capacity (1) 4:15	characteristic (1) 62:15	clear (6) 10:16;11:18;32:14;55:17; 58:4;63:14	compromise (2) 8:14;12:11
Captain (7) 4:6,6;37:12;42:6,10,14; 44:7	characterized (1) 56:15	clearance (6) 24:21,21;25:5;26:10; 36:20;37:3	compromised (12) 8:10;12:20;15:21;24:11; 48:4;53:20;55:16;57:10; 58:7;59:21;63:11;70:1
captured (4) 16:5;56:8;76:19;77:9	Charge (7) 5:5;31:9;70:21;71:1; 73:8;78:19;81:3	clearly (1) 62:5	compromising (1) 12:15
card (2) 9:15;15:15	charged (1) 70:20	Clinton (1) 9:6	computer (29) 14:11,12,15,17;15:6,19; 16:18,19;17:5;20:9;38:18; 47:18;54:2,5;71:6;75:7,10, 11,17,19,20;76:13;78:4,11, 15,17;79:5,14,19
cared (1) 9:3	charges (1) 13:21	closely (8) 10:7;14:8,13,15;29:16; 35:9,15;36:10	computers (12) 14:6,7,8;16:17;28:14; 29:2;31:10;38:18,21;76:7, 11;77:10
carelessness (1) 9:3	chat (5) 40:7;48:10;56:8,10;71:4	closing (3) 5:13;6:15;7:12	concerns (1) 53:18
case (9) 11:17;13:12;15:8;20:3; 59:18;60:3;62:7;70:16; 77:10	chats (15) 9:4;11:5;15:1;46:9;49:7; 50:4;56:18,19;57:3;58:15, 15;59:5;64:3;67:14;68:9	cognizant (1) 11:17	concluded (5) 35:20;52:5;62:14;63:2; 69:1
cases (1) 7:2	Chavez (1) 4:19	coldly (1) 48:10	conclusion (2) 35:20;75:21
casualty (1) 73:5	Chief (8) 27:8;30:16,18;42:6,20; 43:5,16;67:9	collaboration (2) 39:20;40:7	conclusions (2) 45:11;60:12
cataloged (1) 28:5	choose (1) 63:17	collate (2) 41:2,5	conduct (1) 13:4
caught (2) 68:2,6	chooses (1) 21:12	Colonel (4) 31:16;37:1,17;42:18	conducted (10) 29:5;45:10,12;47:17,20; 56:7;62:1;63:4;66:3,5
cause (3) 18:10;28:20;80:20	chose (4) 12:10;63:17;68:3;71:19	combat (1) 10:3	conducting (4) 20:15;30:8;42:7;43:17
caused (3) 13:3;53:10,18	chronological (1) 12:18	combined (3) 22:10;32:20,21	conduit (1) 63:15
CD (3) 20:7;54:2,5	CIA (1) 65:15	command (1) 42:19	conference (3) 6:19,21;7:14
CDs (2) 15:5,6	CIDNE (2) 31:19;39:11	commander (5) 31:16;37:1;44:5;45:3; 81:1	confidence (2) 26:19;27:18
cell (2) 32:12;40:14	CIDNI (1) 15:16	commit (1) 38:5	confidential (3) 18:8,10;20:1
cells (1) 32:7	circumstances (1) 73:4	committed (2) 13:19;27:18	confinement (1) 60:19
Centaur (5) 16:14;77:9,16,17;78:2	civilian (1) 73:4	common (2) 35:14;36:3	confirm (1) 56:10
CentCom (14) 73:2,10;74:1,8,11;76:16, 21;77:12;79:21;80:2,3,4,8; 81:1	civilians (1) 75:16	commonly (2) 39:10,13	confirmed (3) 33:17;50:7;57:4
Center (6) 4:9;49:5,12,21;50:2,7	Class (9) 13:19;17:17;20:12;21:17; 30:4;31:11;48:4,8;74:4	communicate (1) 14:15	Congress (1) 54:11
Central (1) 49:13	classification (5) 18:7;21:11;25:16,19;81:2	communications (2) 54:11;57:21	connected (2) 28:15;75:19
certain (6)	classified (55) 5:12;8:9,15;9:16;10:15; 11:9,13;16:6;18:18,19,19; 19:3,7,14,16,18;20:10;25:3,	community (4) 11:10;14:9;39:21;53:11	connecting (2)
		compiled (1) 30:21	
		complement (1) 17:15	

16:16;79:19 connection (2) 14:13,14 connections (1) 77:11 consequences (1) 9:19 Consider (2) 21:2;35:8 considered (3) 11:3,10;45:20 consolidate (1) 41:15 constant (4) 30:6,7;50:12;55:20 contact (4) 15:11;28:8;46:13,15 contacting (1) 63:6 contained (6) 15:20;26:17;38:19;72:17; 73:12;80:19 containing (2) 46:13;49:13 context (1) 59:2 continue (1) 52:4 continued (4) 63:3;65:19;66:1,20 continuing (1) 40:18 contractors (1) 31:9 contributing (1) 40:15 control (3) 19:4,17;59:7 controlled (1) 64:6 conversations (1) 36:1 convoy (1) 37:20 convoys (1) 43:2 Coombs (10) 5:17,18;6:9,16;7:5,13; 69:17;70:4,8;81:11 copy (9) 6:14,16;15:16;28:12,17, 21;29:7;71:6;74:14 Corp (1) 54:10 corrected (1) 15:13 corrective (1) 33:16 correlating (1) 63:1 correspond (1) 65:6 corresponding (1)	50:10 counsel (1) 6:18 counted (1) 62:21 counter-intelligence (3) 50:19;51:7,13 country (3) 9:5;33:3,9 country's (1) 34:3 coupled (1) 9:1 Court (39) 4:2,2,5,17,18,21;5:1,14, 17;6:5,8,10,12,12;7:1,5,10, 15,16,18,18,19;8:2;13:14; 53:4;69:8,14;70:4,9,9,12, 12,13,14;72:6;76:2;81:9,12, 12 courtroom (2) 4:10,11 Court's (2) 5:21;6:7 covering (1) 14:18 cracking (1) 17:4 create (3) 40:12;41:20;58:13 created (10) 33:21;38:11;46:18;49:4; 50:13;52:21;54:4,16;75:9; 77:15 creates (1) 54:5 credit (1) 22:12 crime (1) 59:17 crimes (3) 13:20;14:19;38:6 criminal (2) 25:21;27:15 crisscrossing (1) 16:15 criteria (1) 61:14 criterion (1) 18:17 critical (2) 20:18;24:10 critiques (1) 61:20 crypt-ed (1) 75:15 Crypto (2) 57:20,20 CSD (1) 9:6 current (4) 43:6,17,21;44:2 currently (1)	4:16 cyber (1) 29:9 D D6A (8) 30:17;31:4,5,7,9;38:18, 18;39:7 daily (3) 24:6;30:20;37:15 damage (2) 18:11;22:8 damaging (1) 10:5 dangers (2) 26:4;51:15 darkness (1) 68:7 data (16) 15:3,4;16:13,14;30:17; 41:2;42:1,6,11;43:17; 45:10;46:5;54:1;64:3;70:1; 77:9 database (4) 31:19;39:14;40:4;69:5 databases (7) 15:17;42:5,8;46:4;50:9; 63:10;64:20 dataset (1) 70:15 date (6) 14:19;15:4;54:2;67:10; 77:2,6 dated (8) 5:3,6,9;16:1;33:20;52:13; 54:8;71:6 dates (5) 34:9,14,20;77:16;79:7 day (8) 10:2;21:6;30:19,21;48:3, 6;49:9;79:10 days (5) 47:21;48:2;49:3;77:18,20 dealt (1) 37:14 December (30) 16:1,1,8;32:3;47:4,11; 51:3;54:11;62:16;65:5,20; 66:2,4,18;67:4,8;68:13; 71:6;72:1,3,9,12;73:19,20; 75:10;76:1,19;77:1;80:11, 12 decisions (4) 18:16;21:11;42:19;44:6 deck (1) 21:9 declassification (1) 19:9 decreased (1) 42:16 decrypting (2) 71:10;75:12	decryption (2) 72:4,14 defeat (2) 32:4;38:11 Defense (17) 5:3,19;6:11;7:6;34:15; 44:12;50:10;55:14;60:8; 63:13;64:14,15,15,21; 71:11;78:6;80:18 definition (1) 34:4 deleting (1) 14:18 deliberate (1) 33:7 deliberately (4) 12:10,20;59:20;67:10 deliberations (1) 14:5 delineated (1) 35:14 delivered (2) 8:16,18 Delta (3) 53:17;66:13,14 demonstrate (1) 12:9 demonstrated (1) 62:10 Department (5) 16:12;34:14;48:5;55:13; 62:20 deployed (7) 8:3,7;38:4,9;45:8;48:15; 60:15 deployment (3) 10:4,10;66:21 Deputy (1) 81:1 described (3) 53:15;57:5;68:20 describing (1) 10:1 description (1) 35:4 designations (1) 18:8 designed (2) 36:17;38:21 desired (1) 44:2 destinations (1) 77:11 destroyed (1) 8:13 destroys (1) 71:13 destruction (1) 28:16 detailed (2) 53:16;68:15 details (1) 73:16
---	--	---	--

detainee (5) 65:20;66:2,8,9,17 detection (1) 20:17 determine (2) 42:15;68:17 detriment (1) 12:5 device (1) 15:10 devices (1) 37:8 devoted (2) 64:18,19 die (1) 68:8 difference (1) 61:8 different (7) 16:16;19:15,21;23:7; 37:18;56:14;75:1 difficult (1) 68:16 digital (2) 19:20;20:3 diplomats (1) 34:15 direct (1) 55:15 discipline (1) 13:5 disclose (5) 21:12;25:14;27:20;64:11; 68:3 disclosed (2) 58:2;59:21 disclosing (3) 11:15;67:6;71:16 disclosure (1) 55:12 disclosures (4) 15:18;20:21;35:21;48:20 discover (1) 20:15 discredit (1) 13:6 discuss (3) 7:1;15:13;21:1 discussed (4) 38:9;50:1;53:11;55:7 discusses (1) 58:7 discussing (3) 54:10;57:9;59:10 disgruntled (1) 24:17 disk (1) 20:4 display (2) 42:13;73:13 disprove (1) 71:12 disseminate (1)	40:9 dissemination (1) 39:9 distant (1) 43:7 diverse (1) 56:2 division (1) 40:10 divulging (1) 35:9 doctrine (1) 15:12 document (18) 18:19;25:17;30:21;50:17, 21:51;7:53;3,21;54:16,17, 19,20;55:17;58:12;68:18, 19,21;80:4 documentaries (1) 35:17 documentary (1) 13:14 documents (15) 8:15,16,19;19:6,6;25:10, 17;27:21;51:18;52:15; 57:11;58:16;59:16;64:19; 72:21 DoD (5) 24:5;51:17;52:2,7;58:7 dog (1) 9:1 domain (2) 58:5,21 donors (1) 64:7 down (2) 40:10;68:8 download (1) 80:3 downloaded (7) 53:6;54:17;79:11,14; 80:4,8,11 downrange (2) 31:6;32:6 draft (1) 61:21 draw (1) 42:17 drive (9) 15:10;28:5,21;29:13,21; 32:18;33:15;46:15;78:9 drown (1) 42:17 Drum (2) 31:12;32:5 duly (1) 81:2 duplicate (1) 75:6 during (10) 9:12;14:1,5;16:8;19:19; 28:1;32:11;33:14;47:6;80:8 duties (1)	17:13 E early (4) 16:14;67:4;68:12;73:18 easily (1) 29:6 easy (1) 28:8 editorial (1) 58:10 editors (1) 63:6 education (1) 12:4 effort (2) 72:5,14 Ehresman (4) 30:4;43:5,16;67:9 eight (1) 4:9 eighth (1) 16:21 either (2) 6:15;79:8 electronic (1) 37:8 elements (1) 56:3 elicited (1) 17:3 Elisa (1) 26:2 else (2) 7:11;49:20 email (4) 6:16;21:1,3;59:11 employ (1) 43:19 employed (3) 39:11;42:11,21 employee (1) 71:5 employees (1) 24:17 employer (1) 75:9 enable (1) 41:2 enabled (1) 41:4 enables (1) 39:20 enabling (1) 29:16 encrypted (3) 71:7;75:19;78:20 end (1) 11:6 ending (1) 16:19 enemies (12)	10:15;20:19;21:13;23:6; 28:3,14;29:18;33:1,8;36:4; 43:11;60:6 enemy (33) 8:17;10:18;11:1,1;13:9; 20:14;22:6,16;23:1,2; 31:21;38:2,11;40:15;41:1,4, 8,16;42:12;43:9,10,13,13, 14,14,18;44:4,11,15;45:3,7, 8,12 enemy's (2) 44:15,20 engine (1) 39:19 enough (1) 32:21 ensure (2) 60:5;68:2 enter (1) 36:21 entered (1) 37:6 enterprise (5) 56:12;59:16;61:5,7,15 enterprises (1) 61:2 entire (4) 15:16;21:9;41:11;79:11 entirely (2) 50:4;61:19 entitled (1) 28:18 entry (1) 78:3 environment (1) 38:9 escort (1) 36:21 essential (1) 44:5 essentially (3) 39:8;51:14;61:12 established (1) 59:16 evaluation (2) 17:21;57:4 even (9) 20:8;34:15;37:1;39:5; 44:14;57:9;61:13;67:9; 71:19 evening (1) 7:4 Event (4) 59:1;67:8,8;71:14 eventually (1) 24:21 everybody (1) 81:10 Everyone (1) 36:19 evidence (27) 9:7;11:17,21;12:3,18; 13:2,8,14,18,21;14:3,4,19;

15:8;16:3,21;17:2;29:13; 33:5;45:20;49:1;62:7,9; 63:14;71:12;76:2,6	exposure (1) 31:12	10,12,14,15,20;79:1,1,4,7, 13,13,15,15;80:15,16	40:14
evidenced (1) 28:3	external (10) 15:9,10;28:5,21;29:12, 21;32:18;33:15;46:15; 55:12	filed (3) 5:1;6:17;22:7	FOIA (1) 6:3
exact (2) 33:11;67:9	extracting (1) 11:14	files (4) 75:12;76:20;79:8,14	folder (4) 54:3;73:9;76:20;78:8
exactly (2) 56:1;60:3	F	Finally (4) 13:7;17:6;20:20;52:5	folders (1) 75:1
examination (1) 33:14		find (2) 11:8;76:6	follow (2) 11:21;63:3
examined (1) 76:8	facilities (1) 34:18	Finding (3) 6:11;32:7;67:6	followed (1) 6:7
examiner (1) 76:5	facility (1) 36:17	findings (1) 31:15	following (2) 22:4;36:1
examiners (1) 14:21	fact (2) 9:1;13:17	fine (1) 6:8	force (1) 51:12
example (3) 22:4,8;62:13	facts (3) 59:19;71:10,15	finished (1) 47:2	forced (1) 13:6
examples (1) 29:2	failed (1) 61:13	finishing (1) 70:6	Forces (3) 45:8,14;51:21
exclusively (1) 63:18	fame (1) 67:19	fire (3) 30:9,9;43:2	forefront (1) 14:4
executed (1) 26:20	family (1) 34:19	fired (1) 48:10	foreign (11) 9:20;18:20;21:13;35:10; 42:4;51:18,19,20;52:6; 68:17,17
Executive (1) 18:14	far (1) 56:17	firewall (1) 16:12	forensic (5) 14:19,21;33:14;76:5,13
Exhibit (67) 5:9,12;6:2;17:1,2,19,19; 18:4;20:6,12;21:9;22:20; 23:21;24:1,2,14;27:1,5; 28:6,9;33:19,20;46:11; 47:16,16,19;49:7;50:8,10, 20;51:1,5,9;52:15;53:1,4,5, 8;54:1,14,15;55:10,19; 56:18;58:14;64:14,15,15; 65:4,13;68:10;73:6,7;74:1, 14,17,21;75:13;76:18; 77:14,15,21;79:2,5,16,18,20	Farah (1) 80:5	firewalls (1) 16:4	forensically (4) 14:17;46:12;73:17;76:12
exhibits (3) 5:1;64:20,21	fast (1) 48:21	first (26) 11:4;12:2;13:19;14:6; 20:12;25:4;30:3,4;31:8,11; 38:13;41:14;47:4;48:4,8; 50:18;51:10;52:16;56:20; 57:5;67:13;70:1,15;74:4; 76:4;77:5	form (2) 60:2;63:10
expected (5) 13:16;26:3;39:18;44:18; 73:15	faulty (1) 62:14	first-class (1) 31:17	formal (4) 12:4;17:18;30:1;32:3
experience (1) 32:16	fear (1) 55:15	firsthand (2) 62:4;63:7	formally (2) 23:9,12
expert (3) 5:7;44:13;60:9	February (9) 48:16;49:5;53:7;54:17; 77:4,8,12;78:1,5	fish (1) 10:5	format (2) 9:6;42:3
experts (1) 73:3	Fein (13) 4:3,4,18;5:2,15;6:6;8:1; 53:5;69:11,20;70:14,15; 72:8	five (7) 47:21;48:2;49:3;51:2; 70:10;74:15,19	forums (1) 36:1
explain (4) 12:3,7,12;71:14	fellow (2) 35:2;37:21	fix (1) 55:6	forward (1) 59:3
explained (7) 14:1;21:17;22:9;26:13; 40:1;42:15;43:5	few (3) 29:2,3;68:7	flag (1) 10:11	found (8) 9:15;20:4;33:15;46:3,12, 12;53:7;75:8
explanation (1) 76:3	Field (7) 28:13;29:1,7;31:5;39:16; 40:10;44:13	flawed (1) 60:11	four (2) 47:20;48:1
exploitation (1) 39:9	Fifth (1) 15:19	flow (1) 16:14	Fourth (2) 15:15;79:2
exploited (1) 41:10	fight (1) 45:15	FOB (7) 32:15;36:15;38:14,15; 48:1,2;78:9	Fox (1) 25:1
exposes (1) 26:8	fighting (1) 71:11	focus (3) 32:11;40:16;44:3	Foxtrot (2) 64:15,21
	figures (1) 32:1	focused (8) 30:5;34:5;40:16;48:13, 14;50:14;65:9;73:3	free (2) 36:5;58:21
	figure's (1) 59:11	focusing (1) 12:14	Freedom (1) 59:3
	file (32) 7:3;16:1;28:9;46:12,17; 54:3,6;55:18;70:20;72:16, 17,17,18;73:7;75:8,19;78:7,	FOG (1)	friendly (1) 32:1

17:15;25:1;32:18;69:13 fully (1) 8:7 Fulton (5) 42:6,10,14,18;44:7 further (3) 28:20;35:14;63:2 fusion (2) 32:12;40:14 future (1) 43:7	governments (2) 35:10;68:17 Government's (2) 5:10,12 grab (1) 22:11 Granai (2) 15:21;71:2 granted (2) 17:12;25:3 grave (1) 70:5 grinning (1) 9:21 group (1) 59:3 groups (5) 22:19;34:14;35:8;43:18; 51:19 Guantanamo (3) 66:13,14,17 guarantee (2) 48:20;67:19 guiding (1) 17:7 Guilty (1) 6:12 guys (1) 31:14	36:16 heads (1) 73:13 heard (12) 13:14;20:3;38:7;39:3; 40:11;44:7,12,21;47:1; 49:1;74:6;78:7 heart (1) 9:7 heat (1) 68:8 held (10) 10:8;14:8,13,15;29:16; 33:6;35:9,15;36:10;54:11 help (1) 22:6 helped (1) 70:17 helping (1) 70:19 helps (1) 71:14 here's (1) 76:4 hey (1) 59:14 high (1) 34:15 highlighted (1) 25:13 highlighting (1) 34:13 highlights (1) 31:14 Hillary (1) 9:6 himself (5) 9:3,12;10:10;28:4;68:5 historic (1) 44:1 historical (2) 43:16,20 hold (1) 33:10 Honor (167) 4:4,7;5:2,11,15;6:6;8:1,2; 9:1,9,15,17;10:17;11:16; 12:2,7,12,17,21;13:2,7,12; 14:6,21;15:9;16:2,8,18; 17:1,1,6,10,20;18:1,7,12,17, 21;19:5,19;20:6,11,20; 21:15;22:18;23:9,18;24:2,8, 14,19;26:2;27:5,11;28:1,7; 29:11;30:3;31:3;32:4,14, 20;33:4,10,18;34:2,4,8,12, 16,21;35:12,19;36:6,13; 37:11;38:7,13;39:3,13,17; 40:11,18;41:13;44:21;45:6, 17;46:8,11,16;47:1,8,17,21; 48:3,11,12;49:1,20;50:18; 51:10;52:1,11,12,16;53:3, 20;54:7,13,14;55:16,20; 56:6,17,19;57:3;58:15;59:5,	9,15;60:3,8,13;61:12,16; 63:12;64:8,17;65:10;66:1,7, 16;67:3,21;68:6,20;69:6; 70:3,8;71:1,11,13;72:13,15; 73:6,17,19;74:14,16,16; 75:3,7,13,18;76:4,15;77:1, 5,13;78:10,16;79:2,16;80:7, 10,12;81:4 hour (1) 69:18 hours (3) 67:3,3;69:13 housed (1) 76:18 human (3) 9:1,2;24:17 hundreds (3) 8:15;9:13;27:20
G			I
gaps (2) 45:2,5 garrison (1) 32:17 gather (4) 33:2;38:16;49:2;64:11 gathering (2) 35:4;42:2 gave (8) 6:13;12:4;33:11,12; 37:12;41:2,10;71:4 gear (1) 8:8 general (3) 11:5;56:21;61:2 generally (1) 42:8 Germany (1) 54:12 gets (1) 6:3 GITMO (4) 53:17;65:12;66:17;67:1 given (3) 22:6;26:11;29:17 giving (2) 13:9;57:15 gleeful (1) 9:20 Global (1) 16:20 goal (1) 58:13 goals (1) 56:14 Golihood (1) 5:6 good (5) 10:2;13:5;44:8;69:6;81:7 Google (1) 39:20 go-to-guy (1) 42:1 Government (25) 5:7;6:1,5;7:3,21;11:10, 14;18:14;19:4,11;25:13; 26:5,20;34:17;50:7,12,14; 53:19;56:5;57:7;59:6; 61:10;63:19;64:5;81:5	H		
	hackers (2) 24:18;35:11 Hall (2) 44:12,21 Hammer (8) 32:15;36:15;38:14,15; 40:14;48:1,2;78:9 hand (2) 26:16;62:16 handle (1) 25:14 handling (1) 31:6 hands (4) 36:11;38:1;72:3,14 happen (1) 43:7 happened (2) 59:18;60:3 hard (9) 15:10;28:5,21;29:13,21; 32:18;33:15;46:15;71:12 harder (1) 59:7 hardware (1) 31:6 harm (3) 8:9;22:12;80:20 head (1) 58:18 headquarter's (1)		IA (1) 24:6 Iceland (8) 47:11;48:9,13,15,16,19; 49:11,19 identification (1) 23:4 identified (4) 14:7;25:11;56:20;64:10 identify (2) 43:11;55:3 identifying (2) 35:2,13 identities (1) 22:19 IED (4) 31:20;32:3,4,7 IEDs (4) 30:8,12,14;43:2 immediate (1) 43:7 impact (3) 24:12;58:12;61:12 imperative (2) 21:20;37:13 importance (3) 24:10;27:12;36:9 important (3) 20:13;43:17;71:3 importantly (1) 80:7 improperly (1) 25:14 inaudible (36) 16:11;20:19;37:17;39:12, 13;42:7,8,20;47:7;48:5; 49:12;51:6,13;54:19;55:2; 59:13;60:9;65:4,9;70:16; 71:8;72:1,10,21;73:1,5,7; 74:12;75:2,6;78:7,8,14,16; 79:3;81:1 inbound (1)

<p>43:6 incident (1) 73:5 include (2) 23:3;34:9 included (4) 24:16;31:19;37:1;44:9 includes (2) 35:15;53:13 including (12) 13:15;22:19;26:18;35:11, 17:37:4;45:18;55:8;60:6; 62:2;73:11;75:3 inclusion (1) 69:4 incorrectly (1) 62:19 increased (1) 42:16 independent (3) 29:4;62:1;63:5 in-depth (1) 44:19 indexdax (3) 79:4,7,18 indirect (2) 13:10;30:9 indiscriminate (1) 8:14 individual (6) 19:13;22:13;25:4,5; 34:19;55:15 individuals (1) 29:4 individual's (1) 22:13 infantryman (1) 37:19 information (165) 10:5,8,15,19,20;11:13,14; 12:10,16,19;14:16;15:1,5,7, 11;17:8;18:1,2,5,8,13,18, 18;19:3,10,14,16,18;20:14, 18;21:12,19,20;22:2,5,10, 11,16;23:4,19;24:5,7,11,11, 15;25:3,6,11,12,14,16;26:6, 8,9,12;27:4,8,13,19;28:9; 29:5,12,14,16,16,17;30:7, 11;33:2,8;34:5,9,10,16; 35:2,10,15;36:1,2,10,11,18; 37:5,9,14,16;38:1;40:9; 41:4,7,12,18,19;42:11,18; 43:20,21;44:2,9,16,20;45:1, 2,14;46:1,2,13,16;48:5; 49:3,8,14,19;51:18,21;52:3, 4,7,13;53:2,13,16;55:8,9, 14;56:1,2;57:10;58:5,8,9, 20,21;59:3,4,7,8,11,12,21; 60:2,5;61:6,11,12,13,17; 63:10,16,20;64:2,6,11,12; 65:12;67:1,18,19;68:1,4,14; 71:17;73:12;75:4;80:19 informative (1)</p>	<p>32:18 informed (1) 68:12 infrastructure (1) 24:10 initial (1) 41:9 Initiative (1) 48:17 inside (2) 58:17,18 insider (4) 46:3;55:13,13,14 insight (1) 60:13 installations (1) 34:18 installed (1) 38:21 instances (1) 28:19 instant (1) 40:8 Instead (1) 37:7 instructed (2) 23:5;68:10 instructing (1) 21:16 instruction (1) 17:20 instructor (1) 21:16 Insurgent (2) 28:12;29:8 insurgents (2) 30:8;51:19 intel (4) 11:6;53:2;57:16;74:5 Intelink (7) 16:7;39:19;40:2,5;46:21; 65:3;66:21 Intelinks (1) 47:9 intelligence (62) 8:11;11:4,10;12:8;13:3, 10;14:9;17:12,14;21:7; 24:19;28:13;29:10;30:2,15, 19,20;31:18;32:17,19;35:4; 36:8,13;37:14,21;38:8,10, 14,16;39:1,4,6,8,21;40:20, 21;41:20;42:2,3;43:4,20; 44:3,13;45:2,4;46:6;49:13; 51:18;52:12,17,18;53:11; 55:21;56:13,20;57:1,6,7; 63:21;64:1,19;65:8 intelling (1) 73:21 intend (3) 12:7,12,17 intends (2) 11:21;12:3 intent (1)</p>	<p>52:10 intentional (1) 33:7 intentionally (3) 12:10,19;59:20 intentioned (1) 9:18 interest (4) 8:5;50:6;56:4;57:8 interested (4) 10:6,9;48:19;71:16 internal (1) 24:16 internet (21) 13:4;21:19,20;22:2,11; 23:1;26:6,8;28:15;29:2,6, 17;33:2;35:17;36:2,11; 52:13;55:7;58:3;62:21;63:9 interrogation (7) 65:15,16,17,21;66:4,14, 18 interrogations (1) 65:12 interview (1) 62:3 into (8) 15:6;30:21;42:4;43:8; 54:5;68:7;75:10,11 introduced (1) 15:7 investigating (1) 73:4 investigation (4) 16:11;73:1,3;79:11 investigations (1) 75:1 IP (1) 16:18 Iraq (9) 8:13;15:11,16;23:13; 32:11;33:5;42:17;43:1; 48:15 IRR (11) 50:16;52:13,16,18;53:2,9, 11;54:16;68:12,20;69:1 Islandic (1) 48:17 ISN (1) 67:1 issue (1) 78:18 issues (2) 7:2;31:7 items (2) 65:3,6 Ivory (3) 26:2,13,21</p>	<p>Jason (4) 15:19;71:5;75:7,8 job (4) 30:5;37:15,16;42:4 jobs (1) 38:8 Johnson (3) 46:12,17;76:5 Johnson's (1) 33:14 joint (1) 32:4 journalism (2) 56:16;61:8 journalist (1) 57:12 journalistic (6) 56:11;59:16;61:1,5,7,14 journalists (1) 36:2 JRTC (4) 30:4;31:13;32:13,16 JTF (1) 66:17 judgment (1) 51:11 Julian (20) 11:3;14:16;15:2;17:3; 46:1,3,13;47:13;48:10,16; 50:1,2,4;56:9,18;57:3,14; 61:20;64:4;68:9 July (5) 5:3,6,9;32:10;60:18 jumped (1) 23:17 June (4) 33:21;35:12,20;36:8 junior (3) 44:14,16,18</p>
K			
<p>Katz (2) 71:5;75:8 Katz's (3) 15:19;75:7,19 keep (1) 28:7 keeps (1) 78:11 kept (6) 28:11,12,17,21;29:7; 67:21 key (9) 12:2;13:21;14:3;15:8; 16:3,21;19:1;33:4;51:11 kind (1) 34:14 Kits (1) 39:7 knew (22) 10:21;11:1,2;12:9,14; 24:4,9,15;25:2;27:12;</p>			
J			
<p>January (9) 9:12;14:18;47:12;54:8; 71:9;75:14,17;76:10;77:3</p>			

29:13;36:10;40:21;44:14; 48:18;56:1,13;58:2;62:8; 67:19;77:18;80:13 Knowing (2) 20:16;60:1 knowingly (2) 13:9;27:16 knowledge (12) 8:9;12:5,13;29:15;33:1; 40:3,21;44:10;45:17;62:4, 12;63:7	leaks (1) 35:14 learn (1) 50:11 learned (9) 19:5,8,12,20;23:10,12,13, 15;28:1 least (3) 51:2;68:8;75:5 leave (4) 37:8;48:4;49:4;77:7 left (2) 37:6;47:6 legal (1) 74:4 lengthy (1) 70:2 less (6) 23:17;46:19;51:2;57:7; 65:1;79:11 lesson (1) 17:20 letter (1) 9:21 level (3) 22:5,9;81:4 light (1) 17:7 likely (1) 52:2 Lim (1) 37:12 limitations (1) 19:1 Line (14) 53:7,21;54:7,16,21; 65:18;66:2,4,6,11,19;67:2; 77:21;79:20 Lines (2) 65:21;66:10 link (1) 14:8 List (15) 16:20;17:7;50:8;57:16; 59:13;64:9,13,14,16;65:3,7, 14;66:7,12;68:1 listed (2) 73:8;78:14 lists (1) 35:7 litany (1) 25:9 little (1) 72:6 live (1) 36:5 lives (1) 24:13 locally (1) 79:8 locate (1) 31:14 located (6)	36:16;72:20;74:13;78:8; 80:5,16 location (2) 22:15;34:17 locations (1) 34:10 log (3) 53:2;54:5;76:19 logged (1) 15:8 logistics (1) 7:1 logs (23) 16:4,7,10,12,15;50:20; 56:8,10;71:4;76:17,17;77:1, 2,9,16,17;78:2,3;79:17,19, 21;80:2,8 Loma (1) 15:2 long (3) 6:6;8:17;69:18 longer (1) 69:8 look (4) 51:9;56:17;57:12;79:16 looked (1) 56:7 Looking (4) 10:4;55:17;64:12;69:10 lowest (2) 22:5,9 lunch (6) 69:10,12,15,19;70:7;81:8	53:5;69:11,20;70:14,15; 72:8 making (2) 10:9;45:11 Manning (174) 8:3;9:2,11,21;10:3,13,18; 11:2,7,18;12:14,19;13:3,8, 19;14:20;15:21;16:15,19; 17:3,11,17;18:3,5;19:2,5; 20:2,7,12;21:10,16;22:1,14, 18,21;23:5,7,9,15;24:9,15, 20;25:2,8,17;26:4,7,13,14, 16,20;27:2,6,16;28:1,4,7; 29:11,21;30:10,15,17,19; 31:1,4,8,12,18;32:12,14; 33:5,11,18;34:1;35:7,14; 36:7,13;37:4;38:3,12;40:13, 19;41:2;42:11,21;44:8,14; 45:6,9,21;46:5,20;47:5,9, 11,18;48:4,8,12,18;49:2,4, 10,18,20;50:1,11;51:1,14; 52:9;53:6,20;54:17;55:16, 21;56:10,12,13,19;57:10, 15,19,21;58:2,4,6,15;59:6, 12,20;60:5,14,18;62:7; 63:11,15,20;64:4;65:1,2,11, 15,19;66:1,9,16,20,21;67:3, 10,14,17;68:1,3,6,12;70:19; 71:3,13,15,21;72:8;73:18, 20;74:4;75:4;76:13;77:5,7; 78:16,21;79:11;80:12 Manning's (36) 8:20;9:8;12:4,8,13;14:11, 12;15:9,15;16:5;17:7;20:5; 21:15;23:19;30:5;32:21; 33:15,16;34:4,12;38:9; 40:12;41:3,21;42:4;45:17; 46:15;56:7;61:3;70:16; 75:20;77:10;78:4,15;79:4, 19 Manual (3) 28:13;29:1,7 many (3) 23:17;31:18;36:4 map (2) 41:19;42:13 March (5) 16:13;51:4;52:13;66:21; 76:11 Marine (1) 54:10 mark (2) 19:6,20 marked (1) 19:7 Martial (1) 6:12 mass (5) 28:15;42:2,11;68:21;72:4 material (4) 21:4;29:21;69:3,4 materials (2) 8:10;28:4	
L		M		
label (1) 20:2 Laboratories (1) 15:20 laboratory (1) 75:9 labs (1) 71:5 lab's (1) 75:10 Laden (1) 23:11 Lamo (8) 46:9;49:6;56:9;58:15; 67:14;70:17;71:3,4 land (1) 72:13 lands (1) 72:3 language (1) 51:14 laptop (1) 14:12 large (3) 34:14;40:15;55:11 largely (1) 60:17 largest (1) 64:16 last (6) 4:5;6:16;7:20;70:1,14; 78:11 late (4) 8:3;16:13;67:4;73:18 later (5) 15:14;48:6;53:2;66:5; 80:12 lead (1) 75:21 leader (1) 46:14 leads (2) 43:15;75:2 leak (3) 11:12;55:14;68:18 leaked (2) 53:12;55:8 leaking (2) 68:19;69:1		Ma'am (4) 5:18;70:15;72:8;81:11 Mac (6) 15:7;54:4,5;72:2,11; 76:12 machine (2) 30:17;39:7 machines (1) 31:7 Madaras (4) 31:3,3;32:9;40:1 Madrid (1) 33:17 magazines (1) 35:16 magnitude (1) 64:17 maiden (1) 22:7 main (1) 61:17 mainly (1) 43:9 maintained (1) 14:9 Major (13) 4:3,4,18;5:2,15;6:6,8;1;		

matter (3) 9:2;33:13;73:3 matters (1) 48:19 maximizing (1) 61:11 maximum (2) 4:15;58:12 may (5) 8:2;25:2;29:9;43:7;55:5 maybe (1) 69:17 McIntosh (2) 14:12;20:9 mean (1) 18:9 meaning (1) 31:2 means (4) 13:10;29:6;47:3;78:16 meant (1) 10:11 measures (1) 19:17 media (7) 4:8,8,10;19:21;20:3; 48:17;62:16 meet (1) 61:13 members (6) 4:8,9;34:19;39:9,20; 41:21 merely (1) 60:4 messaging (1) 40:8 met (2) 6:18;29:5 methodology (1) 60:11 methods (4) 35:3;56:14;68:13;69:3 Microsoft (2) 28:11;78:10 might (2) 7:2;69:6 military (9) 9:20;18:20;22:3;34:6,18; 50:13;56:3;64:19;73:16 Miller (3) 31:16;37:1;42:18 mind (4) 8:20;9:8;14:4;46:3 mine (2) 42:11;50:4 mined (1) 30:15 mining (5) 29:9;30:18;42:1,6;46:5 minus (1) 57:1 minute-by-minute (1) 16:6	minutes (2) 70:2,6 mIRC (1) 40:7 misinformation (1) 60:11 missing (2) 77:16;78:2 mission (5) 8:11;22:15;24:12;61:9; 67:5 mistrial (1) 5:4 mobile (1) 32:3 model (1) 63:3 Modern (1) 48:17 moment (1) 28:10 Monday (1) 7:9 moniker (1) 49:6 monitoring (1) 54:10 month (1) 66:5 months (2) 10:3;60:18 more (14) 10:5;13:13,15;14:2;46:7; 47:10;49:18,19;57:12;59:8; 66:3;69:12,13;72:6 morning (2) 4:8;7:9 Morrow (1) 4:6 Moser (1) 74:10 Most (14) 17:6;43:21;50:8;52:2; 64:9,13,16;65:3,6,14;66:7, 12;68:1;80:7 mother's (1) 22:6 motion (8) 5:3,19,20,21;6:4;7:4,6,9 motions (1) 6:11 Moul (4) 21:15;22:1,21;23:5 Mountain (3) 27:8;36:15;47:3 mounting (1) 15:3 movement (3) 23:4;61:5;73:11 movie (1) 72:18 moving (1) 37:5	much (7) 22:8;42:21;46:1;62:18; 63:16;67:18;69:8 multiple (5) 12:20;16:4;17:16;73:2,10 must (8) 20:16;24:5;34:13;35:3, 21;36:3;52:5;80:10 <hr/> N <hr/> naive (1) 67:7 name (10) 10:9;11:12;22:6,7,12,15; 54:3;64:12;72:16;80:15 named (2) 75:8;78:8 names (2) 34:19;35:1 narrative (1) 71:13 nation (1) 36:12 national (13) 8:5;15:20;18:11;24:12; 26:9;34:6;45:15;50:15; 52:19;56:4;71:5;80:18,20 nationals (1) 21:13 nations (1) 29:4 nation's (1) 36:4 NCIS (1) 50:16 NCOs (1) 34:15 NDA (2) 26:14,21 NDAs (1) 38:3 neatly (1) 29:11 need (4) 7:11;25:5;41:9;75:16 needed (3) 4:14;44:11;71:9 needing (1) 68:7 needs (1) 56:17 net (1) 16:14 network (1) 60:9 networking (1) 35:18 networks (1) 67:15 new (2) 49:21;59:17 news (9)	35:16;49:16;60:17;61:17; 62:11,15;63:1,1,5 newspapers (2) 35:16;63:6 next (6) 28:8;69:15,18,21;70:3; 79:20 night (1) 6:16 NIPRnet (1) 46:4 nondisclosure (8) 25:7,9,20;26:18;27:2,6, 12,17 None (1) 65:7 nor (2) 62:3,9 normal (1) 40:20 note (5) 41:1;51:10,10;74:16; 77:13 noted (1) 57:4 notice (3) 19:2;31:9;75:4 notoriety (2) 8:19;9:5 November (11) 46:18,18;47:3;65:5,5,11, 18;66:10;67:4;73:18,20 NT (2) 78:14,21 number (3) 22:7;23:16;38:7 <hr/> O <hr/> oath (1) 8:4 oaths (1) 10:6 OB (1) 24:7 objection (4) 6:5,7;70:5,8 objectives (1) 67:12 obligations (2) 10:6;27:9 observed (1) 48:8 obtain (4) 27:3,7,19;63:16 obtaining (1) 59:10 obvious (1) 45:21 occasions (1) 51:2 occurred (1) 76:1
--	--	---	---

<p>occurring (2) 30:12;59:2</p> <p>October (1) 8:3</p> <p>off (1) 24:4</p> <p>offenses (1) 5:5</p> <p>offered (1) 60:8</p> <p>office (2) 39:11;74:11</p> <p>officer (1) 44:10</p> <p>official (5) 34:10;37:10;52:14;53:13, 18</p> <p>offset (1) 15:13</p> <p>often (2) 30:12;42:10</p> <p>once (4) 6:10,21;54:4;77:3</p> <p>one (12) 4:9;14:2;21:6;24:4; 30:21;33:4,17;48:3;67:5, 13;69:11;75:21</p> <p>online (2) 68:14;69:4</p> <p>only (18) 8:7;9:2;25:2;26:8;34:10; 37:10;52:14;53:14,18; 55:12;56:17;57:8;62:21; 67:5,8;71:16;74:5;77:2</p> <p>on-the-job (1) 30:1</p> <p>onto (1) 62:20</p> <p>open (6) 36:5;49:4,12,21;50:2,6</p> <p>opened (3) 78:12,16,20</p> <p>opening (1) 14:1</p> <p>openness (1) 58:14</p> <p>operate (2) 43:11,18</p> <p>operated (2) 10:20;62:10</p> <p>operating (3) 16:5;66:13,15</p> <p>Operation (2) 4:9;57:15</p> <p>operational (4) 21:1;34:3;64:3;73:11</p> <p>operations (3) 20:16;30:6;66:17</p> <p>opinion (1) 60:10</p> <p>opinions (2) 60:16;62:6</p> <p>OPSEC (5)</p>	<p>34:4;35:14;36:3;51:13,15</p> <p>oral (3) 7:6,7,8</p> <p>order (16) 4:2;6:7;7:18;11:20;12:18, 21;13:5;18:14;19:18;27:3, 7,18,20;40:19;46:2;70:12</p> <p>orders (1) 64:17</p> <p>organization (8) 11:11;32:5,6;46:6;56:2; 61:9;62:9;63:15</p> <p>organizations (4) 23:8;29:4,9;59:7</p> <p>organize (3) 41:6;42:5,13</p> <p>organized (1) 29:11</p> <p>organizing (2) 41:18;42:3</p> <p>original (2) 57:5;81:2</p> <p>originally (1) 40:4</p> <p>Osama (1) 23:10</p> <p>OSC (3) 49:10,18;50:3</p> <p>others (4) 33:12,12;36:9;66:18</p> <p>out (6) 10:11;19:10;22:12;37:5; 42:5;59:9</p> <p>outcome (1) 10:16</p> <p>outing (1) 57:17</p> <p>outline (2) 13:2,7</p> <p>outside (3) 37:8;62:11;63:5</p> <p>over (6) 7:4;23:15;41:16;42:16; 43:19;62:20</p> <p>Overall (1) 69:12</p> <p>overflow (2) 4:12,14</p> <p>oversight (1) 58:10</p> <p>own (13) 9:4;11:2;12:13;15:12; 22:4;34:12;44:16;45:13; 46:8;56:21;61:3;67:12; 68:16</p> <p>owned (2) 19:3;25:12</p> <p>owners (1) 55:5</p>	<p>41:7,10</p> <p>page (23) 21:3;46:9;50:4;55:10; 56:19;57:3,13,16,17,20; 58:18,21;59:4,9,14;61:21; 68:9;71:4;74:12,15,16,20; 75:16</p> <p>pages (1) 74:18</p> <p>panel (1) 4:10</p> <p>Papa (2) 64:15,21</p> <p>paralegal (1) 74:10</p> <p>parochial (1) 57:7</p> <p>part (2) 72:21;81:6</p> <p>particular (5) 20:13;31:20;39:14;41:15; 42:2</p> <p>particularly (2) 42:12;55:4</p> <p>parties (6) 4:3,4;6:13;7:1,19;70:13</p> <p>pass (1) 76:13</p> <p>passed (1) 24:9</p> <p>password (3) 17:4,4;71:20</p> <p>past (2) 23:16;58:9</p> <p>patten (1) 30:13</p> <p>pattern (1) 31:20</p> <p>patterns (1) 43:11</p> <p>PE (1) 65:18</p> <p>PE81 (1) 65:21</p> <p>Peninsula (2) 13:11;29:19</p> <p>people (1) 57:6</p> <p>percent (1) 62:19</p> <p>period (3) 41:17;43:1;73:19</p> <p>permitted (1) 25:10</p> <p>person (5) 22:11;25:2,6;63:7;72:3</p> <p>personal (13) 14:11;15:7;20:8;21:3; 24:16;29:2;37:7;54:4; 61:21;72:2,11;76:10,12</p> <p>personnel (1) 34:6</p> <p>pertaining (1)</p>	<p>48:19</p> <p>pertinent (1) 10:4</p> <p>Pfc (204) 8:3,20;9:2,8,11,21;10:3, 13,18;11:2,7,18;12:3,7,12, 14,19;13:3,8;14:11,12,20; 15:9,15,21;16:5,15,19;17:2, 7,10,16;18:2,5;19:2,5;20:2, 4,7;21:10,15,16;22:1,14,18, 21;23:5,6,9,15,19;24:9,15, 20;25:2,8,17;26:4,7,13,14, 15,20;27:2,6,16;28:1,4,7; 29:11,21;30:4,10,15,17,19; 31:1,4,8,11,18;32:11,14,21; 33:5,10,15,15,18;34:4,12; 35:7,14;36:7,13;37:4;38:3, 9,11;40:12,13,19;41:2,3,21; 42:4,11,20;44:7,14;45:6,9, 17,21;46:5,14,20;47:5,9,11, 17;48:12,18;49:1,4,9,17,20; 50:1,11;51:1,14;52:9;53:6, 20;54:17;55:16,21;56:7,10, 12,13,19;57:10,15,19,21; 58:2,4,6,15;59:5,12,20; 60:4,14,18;61:2;62:7;63:11, 14,20;64:4;65:1,2,11,15,19; 66:1,9,16,20,21;67:3,10,14, 17;68:1,3,6,12;70:16,19; 71:3,13,15,21;72:8;73:18, 20;75:3,20;76:13;77:5,7,10; 78:4,15,16,21;79:4,11,18; 80:12</p> <p>phase (1) 5:11</p> <p>phone (2) 57:20,20</p> <p>photos (1) 66:8</p> <p>physical (1) 13:13</p> <p>pick (1) 31:13</p> <p>picture (6) 9:9,9,10,11,14,17</p> <p>piece (5) 15:8;16:3,21;23:2;33:4</p> <p>pieces (2) 13:13,21</p> <p>piecing (1) 44:16</p> <p>PII (1) 64:3</p> <p>PIR (1) 45:1</p> <p>place (2) 8:5;19:17</p> <p>placed (2) 26:19;60:18</p> <p>plan (3) 14:20;17:21;22:16</p> <p>plans (2) 17:20;18:20</p>
	<p>P</p>		
	<p>packaged (2)</p>		

<p>platform (2) 8:17;60:4</p> <p>play (2) 24:5;43:8</p> <p>played (1) 38:12</p> <p>please (5) 4:3;8:2;41:1;46:1;51:10</p> <p>pledged (2) 27:2,7</p> <p>plot (1) 41:19</p> <p>plug (1) 75:10</p> <p>pm (1) 81:13</p> <p>point (2) 51:10;62:5</p> <p>policy (1) 9:20</p> <p>political (3) 32:1;58:12;61:11</p> <p>poor (1) 62:12</p> <p>portal (3) 54:21;74:15;78:5</p> <p>portion (2) 12:1;15:16</p> <p>posed (2) 51:8;61:1</p> <p>poses (1) 50:15</p> <p>position (1) 26:12</p> <p>posses (1) 55:11</p> <p>possession (3) 19:10;29:12;52:3</p> <p>possible (3) 11:7;46:1;48:21</p> <p>post (4) 52:4;59:17;60:17;68:14</p> <p>posted (5) 6:4;29:17;52:8;54:20; 61:21</p> <p>posting (6) 21:2;22:5;36:2;52:14; 59:12,13</p> <p>posts (1) 58:9</p> <p>potential (3) 25:13;51:12;55:3</p> <p>potentially (1) 51:20</p> <p>PowerPoint (1) 28:11</p> <p>PPI (1) 23:3</p> <p>precise (1) 27:15</p> <p>precisely (1) 46:7</p> <p>predicting (1)</p>	<p>43:13</p> <p>predictive (6) 40:16;43:9,12,15;44:4,19</p> <p>prejudicial (1) 13:5</p> <p>prepared (4) 6:11,15;42:17;43:1</p> <p>preparedness (1) 73:16</p> <p>present (7) 4:5,6,20;7:19,20;70:13,14</p> <p>presentation (1) 33:16</p> <p>presented (3) 17:18;21:9;33:17</p> <p>presentencing (2) 5:8,11</p> <p>presumed (1) 52:6</p> <p>pretrial (1) 60:19</p> <p>prevent (1) 20:21</p> <p>previous (1) 32:13</p> <p>previously (1) 17:10</p> <p>primarily (1) 38:15</p> <p>principled (1) 57:6</p> <p>principles (1) 24:6</p> <p>printout (1) 55:18</p> <p>prior (4) 10:10;14:19;76:1;80:11</p> <p>priority (1) 45:1</p> <p>Private (5) 13:19;20:12;48:4,8;74:3</p> <p>probably (3) 69:11,21;70:1</p> <p>procedures (2) 66:14,15</p> <p>proceed (2) 7:12,21</p> <p>PROCEEDINGS (1) 4:1</p> <p>process (9) 6:1;18:12;19:9;38:12; 40:13;41:14;42:1;43:5; 62:14</p> <p>processing (1) 39:8</p> <p>produced (2) 19:3;64:9</p> <p>product (6) 12:8;30:13;36:6;43:5; 44:3,3</p> <p>products (2) 38:10;40:12</p> <p>professionals (1)</p>	<p>52:17</p> <p>Professor (13) 60:8,10,13,16,21;61:4,14, 16;62:1,6,13;63:4,12</p> <p>program (2) 17:20;38:19</p> <p>programs (5) 35:16;38:18,21;39:10; 40:6</p> <p>prohibitions (1) 18:21</p> <p>Propaganda (1) 28:12</p> <p>proper (1) 18:15</p> <p>properly (3) 19:6,20;81:3</p> <p>proposed (1) 5:16</p> <p>Prosecution (58) 17:1,2,19,19;18:3;20:6, 11;21:9;22:20;23:21;24:1, 2,14;25:21;27:1,5;28:5,9; 33:18,20;46:11;47:16,16, 19;49:7;50:8,20,21;51:5,9; 52:15;53:1,21;54:13,14; 55:10,18;56:18;58:14; 64:13,20;65:4,13;68:10; 73:6;74:1,14,17,21;75:13; 76:18;77:13,15,21;79:2,5, 16,18</p> <p>protect (17) 8:5;10:7;19:14,18;20:13, 16,19;24:7;34:9,13,15;35:1, 3;36:3;37:16;68:11,11</p> <p>protected (2) 23:3;71:20</p> <p>protecting (5) 27:13;34:3,17,19;36:9</p> <p>protection (3) 24:10;34:5;51:12</p> <p>protective (1) 8:8</p> <p>prove (2) 13:8;32:21</p> <p>proves (1) 33:6</p> <p>provide (3) 37:19;51:18;63:20</p> <p>provided (2) 10:21;41:7</p> <p>provides (3) 34:2;60:11;69:2</p> <p>providing (2) 49:16;56:1</p> <p>proving (1) 13:3</p> <p>public (10) 11:5;34:5;36:1;48:7; 53:14;56:21;58:5,21;59:11; 81:6</p> <p>publications (1) 49:15</p>	<p>publicly (3) 53:12;55:7;67:20</p> <p>publish (2) 5:20;64:5</p> <p>published (6) 6:1;13:4;48:6;53:14; 55:9;58:3</p> <p>publishing (1) 53:16</p> <p>pull (4) 30:10;41:12,14;42:5</p> <p>pulled (2) 45:10,21</p> <p>pulling (1) 44:9</p> <p>purported (1) 63:9</p> <p>purpose (8) 26:14;35:9;42:14;51:6; 52:18;53:9;55:3;61:11</p> <p>purposes (1) 37:10</p> <p>pursuit (1) 67:12</p> <p>put (11) 6:3;19:2;20:7;22:2,10; 30:11;31:8;43:14;48:9; 54:5;75:3</p> <p>puts (1) 26:10</p> <p>putting (2) 26:5,7</p> <p>Pv2 (1) 33:21</p>
Q			
<p>qualified (1) 44:13</p> <p>quick (1) 70:5</p> <p>quickly (2) 40:8;63:8</p> <p>quote (2) 11:5,6</p>			
R			
<p>R&R (3) 48:4;49:4;77:7</p> <p>raise (2) 52:19;53:9</p> <p>raised (1) 26:16</p> <p>ramification (1) 25:13</p> <p>range (1) 28:14</p> <p>ranked (1) 42:5</p> <p>ranking (1) 34:15</p> <p>rather (3)</p>			

67:10;69:19;71:15 raw (1) 52:18 RCM (1) 6:19 reach (1) 42:4 read (6) 6:18;7:10;19:6;31:13,18; 58:7 reader (1) 64:10 readily (2) 38:20;45:19 reading (2) 6:3;21:4 ready (3) 7:21;8:16;41:10 real (1) 48:20 realized (1) 63:8 rear (1) 37:20 reason (4) 20:20;21:5,18;77:8 reasonable (1) 76:3 recalled (1) 48:9 receive (3) 10:19;40:9;58:10 received (10) 17:15,18;18:3,5;21:6; 24:3;30:1;32:2;60:2;61:20 recent (1) 51:16 recess (12) 7:15,17;69:7,10,12,15; 70:6,9,11;81:8,12,13 recessed (3) 4:5;7:20;70:14 recognized (1) 34:21 reconsideration (2) 5:4;6:17 record (3) 6:19;7:19;70:13 records (2) 79:7,7 recount (1) 12:2 recounted (1) 21:16 recover (1) 15:1 recoverable (1) 76:9 recruiting (1) 23:13 red (3) 20:21;74:18,18 redacted (1)	62:16 redeploy (1) 42:17 redirects (1) 74:5 reference (2) 28:8;29:20 referenced (2) 54:9;78:6 references (1) 32:19 reflect (1) 7:19 reflected (1) 79:13 regard (1) 5:18 regardless (2) 60:12;63:12 region (1) 41:16 regular (1) 65:2 regularly (2) 38:19;39:15 Regulation (4) 18:6;19:16;28:17,18 Regulations (1) 18:15 reimaged (1) 76:11 relate (1) 48:15 related (7) 26:9;30:7;47:12;53:2; 65:12;67:5;79:3 relates (3) 13:20;53:6;80:18 relating (2) 42:12;46:6 relations (1) 18:20 relationship (3) 45:18,19;65:7 release (8) 17:9;22:15;48:7;53:17; 60:1;63:8,16;67:20 released (4) 46:2;52:10;58:8;62:19 releases (2) 51:17;63:4 releasing (2) 33:7;36:10 relies (1) 41:5 remain (1) 14:4 remaining (1) 12:1 remember (2) 17:18;21:5 remembers (1) 67:9	remnants (1) 76:6 remotely (1) 79:8 remove (1) 37:9 repeatedly (1) 58:7 repercussions (1) 55:15 report (22) 50:16,19;51:1,5,11;52:5, 17,17;53:7,15;54:8,9,13; 55:3,6,11;58:6,11;62:11; 68:12,15 reported (3) 56:3;62:19;78:1 Reporter (2) 4:18;5:1 reporting (2) 30:20;62:12 Reports (13) 9:14;31:2,13;39:15; 49:13;50:14;52:9;55:21; 62:3;63:1,1,5;64:1 representative (1) 31:5 represents (1) 51:12 reputation (1) 22:13 request (3) 5:19;6:17;7:6 requested (1) 36:20 required (11) 24:20;25:15,18;30:6,10; 31:1,13;35:1;36:19,21;42:8 requirements (2) 5:21;45:2 research (6) 12:14;30:6;56:6;59:3; 62:2;63:5 researched (3) 8:17;33:21;62:11 resource (1) 11:2 response (2) 7:3;48:6 responsibilities (3) 17:13;26:17;32:13 responsibility (3) 19:13,13;37:8 responsible (4) 31:6;37:4;40:14;68:18 responsibly (1) 62:15 rest (1) 14:14 result (3) 10:17;25:21;27:14 resulted (1) 10:14	retained (1) 28:4 retention (3) 65:16,17,20 returning (2) 48:3;49:4 revealed (1) 9:4 revealing (1) 62:7 reveals (1) 73:16 revelation (1) 57:8 review (4) 52:6;55:21;60:17;74:16 reviewed (2) 61:18;76:16 reviewing (1) 30:7 rifle (1) 8:8 right (15) 4:17,21;6:8,10;7:15; 26:16;46:3,8;47:6;69:6,8, 21;70:4,18;81:9 rip (1) 47:2 risk (1) 26:11 roadmap (2) 12:1;34:2 Robert (1) 4:19 role (3) 24:5;38:11;40:12 room (1) 6:3 rotation (2) 30:4;32:11 rotations (1) 32:16 routine (1) 24:6 rule (2) 6:11;30:20 ruled (1) 6:13 Rules (1) 6:12 ruling (3) 6:14,18;7:10 running (1) 76:7
S			
S2 (7) 30:11;31:15;36:14,15; 37:3,12;39:10 Sadler (1) 39:3 safe (1)			

24:5 safeguard (2) 26:12;38:1 salutation (1) 10:2 same (10) 9:12;15;16:10;27:19; 43:18,19;47:13;49:6,9; 51:14 sanitized (1) 37:3 sat (1) 76:20 saved (2) 15:16;29:21 saw (3) 11:9;56:11,12 scale (1) 40:15 scene (1) 80:17 schedule (3) 5:10,16,16 scheduled (1) 7:7 scheduling (1) 7:1 SCI (1) 24:21 SCIF (3) 36:21;37:9,10 scoured (1) 11:7 scrape (1) 10:5 screen (2) 74:15,21 SD (2) 9:15;15:15 search (8) 39:19;40:5;46:21;49:10; 65:3;66:5,20;67:1 searched (12) 37:7,11;47:9,11,13; 49:18;65:16;66:9,16,21; 67:18;73:20 searches (12) 16:7;47:15,17,20;48:1, 15;50:12;55:20;65:5;66:3; 74:3,5 searching (6) 48:13;65:11,19;66:1; 67:5,21 Second (9) 14:11;27:6;32:11;43:4,8; 47:3;51:16;52:12;76:15 secret (15) 18:9,9,10;20:1,1,5,6,10; 24:20,21;36:20;74:19; 80:17,21;81:4 secrets (1) 36:4 Section (11)	36:14,15;37:13;39:10; 64:16,18,19;69:12,18;70:2, 3 secure (1) 57:21 security (20) 8:5;18:2,2,6,11;22:7; 24:12;25:4;26:9,10;34:3,7; 37:2,20;45:15;50:15;52:20; 55:4;56:4;80:20 seek (1) 49:20 seeking (1) 64:5 selected (1) 62:16 self-interested (1) 10:14 semi-classified (1) 59:15 senior (3) 45:9,10;74:10 sense (1) 36:3 sensitive (3) 51:17;52:2,7 sent (3) 6:16;52:9;58:20 sentencing (1) 5:16 separate (5) 22:7;25:8;51:2;74:8,9 Sergeant (6) 30:3;31:11,17;33:17; 39:3;55:2 serious (2) 18:10;80:20 server (10) 16:10,12;72:10;74:8,8,9, 13;76:17,17;77:12 servers (1) 16:4 service (1) 16:16 services (2) 13:5;51:19 session (3) 69:15,18,21 set (2) 21:10;70:1 setting (1) 59:15 seven (1) 16:18 several (5) 60:18;61:1;64:17;69:3; 73:21 SF312 (1) 25:7 Sgt (1) 31:3 share (1) 75:1	shared (1) 78:9 SharePoint (10) 16:10;74:8,12,13;76:17; 77:12;79:12,19,21;80:4 Shaver (15) 47:8;49:9,17;50:21; 52:21;54:15;72:16;74:6; 75:6;76:5,15;77:14;78:3, 13;79:6 Shaw (1) 4:19 sheet (1) 73:8 Shia (2) 40:16,17 shoe (1) 20:5 shot (1) 30:11 shots (2) 74:15,21 show (7) 16:7,15;40:20;70:13; 77:11;78:21;80:2 showed (8) 23:20;29:15;49:7;64:4; 66:12;77:2,19;78:1 showing (3) 16:11,12;17:2 shows (9) 15:4;53:6;54:16;64:8; 65:14;66:8;74:5;77:16; 79:18 side (2) 37:20;80:2 SigAct (2) 15:16;31:12 SigActs (8) 9:16;10:1;30:16;31:19; 39:15;42:9,12;43:1 sight (1) 37:5 SIGIT (1) 39:4 sign (1) 26:15 signature (1) 30:5 signed (6) 9:21;25:6,8,17,17;38:3 Significant (2) 9:13;39:16 signing (1) 27:11 similar (4) 32:12;39:19;40:7;42:21 Similarly (1) 22:14 simple (1) 10:7 simply (1) 67:7	SIPRnet (40) 11:8,9;14:6,7,10,13;15:6; 16:5,9,16,17;17:4,8,12; 38:15,17,21;39:19;46:3,5, 19,20;47:5,18;49:2;51:3; 54:2,21;63:21;65:2;71:19; 73:21;76:10;77:10;78:4,15, 17;79:4,14;80:16 site (5) 4:13;72:21;79:12;80:3,4 sitting (1) 47:6 six (1) 10:3 sixth (2) 16:3;52:1 SJA (4) 74:1,4,11;75:1 skills (2) 12:4;42:21 slide (36) 18:4,4,7,12,17,21;19:5,8, 12,15,17,20;20:14,18,20; 21:8,8,10;23:9,12,13,15; 24:3,8,14;33:20;34:2,3,8, 12,17,18,21;35:3,12,19 slides (2) 21:10;22:20 slip (1) 68:7 slowly (1) 72:7 small (2) 30:9;43:2 Smith (1) 20:4 social (2) 22:7;35:18 society (1) 36:5 software (2) 31:7;68:16 soldier (9) 9:19;25:15;26:10;36:7; 37:2,6,19;47:6;67:7 soldiers (7) 21:21;35:1,2,21;36:3; 37:11,14 soldier's (1) 22:6 soldiers' (1) 34:19 solely (2) 39:5;68:4 solider (3) 37:4;39:4,5 someone's (1) 22:12 soon (1) 46:7 SOP (3) 53:17;66:17,17 sought (3)
---	---	---	---

10:20;63:18;64:11 source (12) 11:7;17:11;39:1,4,6;49:5; 12,21;50:2,6;57:16;68:11 sources (3) 41:15;49:2;61:17 sourcing (1) 57:2 Southeast (4) 40:17;48:14;57:21;65:8 spanning (1) 43:1 speak (1) 72:6 speaking (1) 41:13 special (21) 8:12;20:3;26:19;27:17; 38:20;41:5,12;47:8;49:17; 50:21;52:21;54:15;72:15; 74:6;75:6;76:4,15;77:14; 78:3,13;79:6 specialized (2) 11:12;32:15 specific (7) 13:20;23:6;37:15;40:2; 42:12;45:5;73:12 specifically (14) 11:3;18:2;19:12;23:10; 24:17;29:18;35:7;38:12; 45:12;50:13;58:19;64:18; 65:10;73:21 Specification (3) 5:4;70:21;71:1 specifications (2) 13:20;14:2 spectators (2) 4:11,11 speculation (1) 8:21 spent (3) 14:2;62:18;67:3 spies (1) 24:18 spread (1) 74:19 spy (1) 57:17 standard (2) 66:13,15 standards (1) 19:16 stark (1) 8:8 start (1) 71:18 started (1) 76:19 starting (1) 51:2 starts (1) 70:16 state (5)	8:20;9:8;16:12;48:5; 62:20 stated (5) 17:10;26:16;50:3;58:13; 59:1 statement (1) 10:10 States (56) 5:15;8:6;10:16;11:9,11, 17,21;12:3,6;13:9,13;14:1, 3;18:13;19:4,11;21:14; 23:3,19;25:12;26:20;28:2, 14,18;29:1,8,18;33:1;35:6, 9,13;39:1;41:5,11;45:14,16; 48:9,14;50:12,13,16;51:14, 16;52:1;53:19;55:11;56:4; 60:7;63:13,19,19;64:18; 65:8;75:14;80:18;81:5 stating (1) 35:21 status (1) 25:16 stay (1) 58:17 steal (1) 16:20 stenographer (1) 4:9 step (3) 41:14;43:4,8 steps (2) 40:19;41:9 sticker (2) 20:5,6 stickers (1) 19:21 stipulation (3) 26:3;39:18;73:15 stipulations (2) 13:16,16 stood (1) 26:16 storage (1) 15:10 store (3) 15:11;19:15;36:17 story (1) 9:9 strikes (1) 75:15 strong (1) 62:5 structure (1) 54:3 struggling (1) 9:19 student (1) 17:21 study (1) 43:10 subject (3) 8:21;33:12;73:2 submission (1)	69:3 submitting (1) 69:4 substantive (1) 57:9 successful (1) 15:17 suggestions (1) 69:2 suite (2) 38:20;41:1 summaries (2) 30:19;31:18 summary (12) 41:20;47:17;50:20;53:1, 5,54:15;65:13;77:15;79:3, 17,20;80:6 super (3) 75:11,16,20 supplement (1) 5:12 support (1) 31:5 sure (1) 27:9 surrounding (1) 73:4 sworn (1) 8:4 system (5) 38:14,18;39:5,14;58:17 systematic (1) 55:21 systems (9) 11:14;18:20;24:7,11; 38:10;41:12,13;67:11; 73:12	44:9 taught (5) 22:1,14;23:6;36:9;51:15 teach (1) 32:5 team (1) 32:4 tells (1) 21:10 ten (1) 78:11 tend (1) 43:18 ten-minute (1) 7:14 term (7) 11:12;47:9,20;48:1; 65:17;66:9,9 terms (3) 18:1;49:10;74:1 terrorism (1) 23:7 terrorist (3) 22:19;23:7,16 terrorists (6) 23:14;24:18;28:19;35:10; 36:12;51:19 test (1) 24:9 testified (39) 17:16;22:21;26:2;27:10; 30:16,18;31:4,11,17;32:2; 37:12,17;39:7,18;41:21; 42:7,10,20;43:16;47:8;49:9, 11,17;51:6;54:20;55:2; 61:16;72:16;73:10;74:12; 76:6,16;77:14,18;78:4,13; 79:6,10;81:3 testifying (1) 62:18 testimony (11) 13:15,16;26:3;39:18; 40:11;47:1;60:21;73:14,15; 77:17;78:7 Thanksgiving (3) 46:9;65:11;70:18 theater (2) 31:8;46:7 thinking (1) 60:14 Third (3) 15:9;54:7;78:6 though (1) 20:8 thought (2) 12:15;62:8 thoughts (1) 56:8 thousand (1) 9:10 thousands (3) 8:15;9:13;27:21 threat (12)
		T	
		tactical (2) 39:15;44:6 tactics (1) 43:19 tag (1) 31:1 tags (1) 9:1 talk (3) 28:9;38:13;53:3 talked (3) 22:4;57:15,17 tampering (1) 28:19 target (1) 17:8 targeted (1) 30:14 targeting (1) 51:21 task (2) 39:2;42:14 tasks (1)	

<p>11:11;43:6;50:15;51:7; 52:19;53:10,15;55:4,4,12; 56:3;77:9</p> <p>threats (2) 24:15,17</p> <p>three (5) 25:3,6;43:1;50:13;64:1</p> <p>throughout (3) 8:21;13:12;66:20</p> <p>thus (4) 14:18;27:17;78:20;80:20</p> <p>timeframe (3) 16:14;46:9;47:14</p> <p>timelines (1) 30:11</p> <p>times (11) 16:8;34:9;47:10,12; 49:19,19;59:17;73:21; 74:19;78:11;79:8</p> <p>timing (1) 71:12</p> <p>Title (1) 28:12</p> <p>titled (4) 28:13;52:13;55:18;78:7</p> <p>today (6) 5:20;6:4,15,20;33:10; 38:6</p> <p>together (4) 23:2;30:11;44:16;45:20</p> <p>told (2) 31:5;59:6</p> <p>tomorrow (1) 7:4</p> <p>took (1) 41:8</p> <p>tool (1) 40:7</p> <p>tools (3) 41:1,3,5</p> <p>top (7) 18:9;20:1;24:21;36:20; 74:17,19;80:17</p> <p>topic (3) 40:3;41:15;42:2</p> <p>topics (2) 47:12;67:5</p> <p>total (1) 47:2</p> <p>track (1) 78:11</p> <p>tracks (1) 14:18</p> <p>traditional (2) 56:15;62:15</p> <p>trailer (2) 4:12,15</p> <p>trained (10) 20:12;22:18,21;24:19; 30:17;32:9;36:7;40:15; 45:6,12</p> <p>training (25) 10:17;12:4;15:12,13;</p>	<p>17:15,18;18:5;21:6;22:20; 23:18,20,21;24:3,4,8;28:4; 29:20;30:1;31:4;32:3,4,15; 33:11,12,16</p> <p>transaction (1) 80:3</p> <p>transfer (1) 14:15</p> <p>transferred (3) 58:16;72:1,10</p> <p>translation (1) 49:14</p> <p>transmission (1) 75:21</p> <p>transmissions (1) 12:21</p> <p>transmittal (1) 9:21</p> <p>transmitted (2) 9:13;80:11</p> <p>transmitting (1) 70:20</p> <p>transparency (4) 59:14;61:5,10;64:12</p> <p>transparent (1) 61:19</p> <p>treated (1) 75:5</p> <p>trend (4) 43:9,10,14;44:4</p> <p>trends (2) 43:11,14</p> <p>trial (3) 8:21;27:15;78:6</p> <p>trip (1) 54:9</p> <p>troop (1) 73:11</p> <p>trophy (1) 15:17</p> <p>troubled (1) 9:18</p> <p>true (2) 10:11;25:4</p> <p>trust (10) 8:12,13;26:12,19;27:18; 37:13,13,17,19;67:11</p> <p>trusts (1) 37:21</p> <p>truth (1) 57:8</p> <p>try (1) 59:8</p> <p>T-SCIF (6) 36:15,17,19;37:3,6;38:5</p> <p>TTPs (1) 28:12</p> <p>turned (1) 10:11</p> <p>tweet (2) 75:14,18</p> <p>tweeted (1) 71:8</p>	<p>twice (2) 24:9;77:3</p> <p>two (14) 13:16;14:7;16:8,16;25:5, 8,17;27:11;32:16;46:19; 47:4;51:3;65:1;69:13</p> <p>txt (1) 55:18</p> <p>type (11) 10:20;12:18;18:18;34:8; 56:1;64:2,10;72:19;78:12, 15;80:19</p> <p>types (2) 12:9;19:21</p> <p>typically (1) 40:2</p>	<p>37:10</p> <p>unprecedented (1) 67:15</p> <p>unredacted (1) 63:9</p> <p>unsorted (1) 64:14</p> <p>untraceable (1) 68:21</p> <p>up (6) 9:9;31:13;40:10;70:6; 73:13;78:21</p> <p>updates (1) 49:17</p> <p>uploaded (2) 72:2,11</p> <p>upon (1) 43:13</p> <p>usable (1) 42:3</p> <p>USC (2) 5:5;25:21</p> <p>use (14) 8:17;22:16;23:2,2;28:19; 30:17;34:10;35:5;36:3; 44:20;45:13;52:14;53:13, 18</p> <p>used (26) 4:16;11:1;12:5;14:14; 16:20;22:3;23:1;33:1,3; 38:10,14,15,19;39:13;40:2, 6;42:18;49:2,5,6;51:15; 52:17;60:5;61:2,19;68:13</p> <p>useful (2) 13:18;43:20</p> <p>user (3) 17:4;78:14;79:1</p> <p>uses (1) 68:16</p> <p>USF-I (1) 16:20</p> <p>using (6) 22:20;46:8,20;49:10; 65:2;76:13</p> <p>utilities (1) 60:12</p> <p>utility (1) 60:20</p>
		<p>U</p>	<p>ultimately (5) 6:3;12:5;21:13;24:13; 31:15</p> <p>unable (1) 78:20</p> <p>unauthorized (1) 51:17</p> <p>uncensorable (1) 68:21</p> <p>uncertain (2) 25:15,18</p> <p>unclassified (3) 20:1;49:14;53:18</p> <p>under (9) 6:12;18:14;19:4,20; 25:21;51:11;59:18;73:9; 78:14</p> <p>understood (7) 20:2;21:21;27:9;28:2; 29:14;36:8;45:7</p> <p>undisputed (1) 71:10</p> <p>unfettered (1) 10:14</p> <p>uniform (1) 36:7</p> <p>unit (9) 8:4;23:3;32:2,9;37:18; 38:9;41:21;42:17;54:20</p> <p>United (48) 5:15;8:6;10:16;11:9,11, 17,21;12:3,6;13:9,13;14:1, 3;18:13;19:4,11;21:14; 23:3,19;25:12;26:20;28:2; 29:18;33:1;35:5,9,13;39:1; 41:5,11;45:14,15;48:8,13; 50:12,13,16;51:13;53:19; 56:4;60:7;63:13,19,19; 64:18;65:7;80:18;81:4</p> <p>units (2) 22:17;32:6</p> <p>unit's (1) 22:15</p> <p>unless (1)</p>
			<p>V</p>
			<p>vaguely (1) 67:9</p> <p>valuable (1) 32:18</p> <p>values (1) 61:18</p> <p>varies (1) 44:2</p> <p>various (1) 41:15</p> <p>vehicles (1) 35:5</p>

versions (1) 64:13	13:3	72:2,4,11;75:14,18	zone (1) 8:4
versus (1) 44:2	wants (1) 59:8	WikiLeaks' (3) 50:6;56:14;68:1	0
via (1) 8:17	war (3) 8:4;14:13;28:3	WikiLeaksorg (1) 55:11	09 (5) 46:18,18;51:3;65:6;68:13
video (36) 15:21;20:4,9,9;59:1,2; 70:20;71:2,7,10,19,20,21; 72:1,9,10,17,19,20;73:10, 15;76:1;77:2,6,8;78:7,19, 19;79:13;80:8,10,13,17,19; 81:3,5	warfare (1) 29:5	Wikipedia (1) 68:21	0930 (1) 7:9
videos (17) 35:18;65:15,16,17,20,21; 66:2,4;73:9;74:12;75:2,15; 76:7,7,18;79:12;80:13	Washington (1) 59:17	willing (1) 72:4	1
view (2) 31:20;62:5	watch (1) 71:20	Windows (4) 72:18,18;78:11;79:9	1 (10) 16:8;18:4;33:20;47:10; 51:3;71:21;72:9;76:19; 77:1;80:11
viewed (3) 51:1;78:21;79:1	watched (1) 59:2	wipe (1) 76:13	1:30 (1) 81:13
violate (2) 27:3,7	way (5) 11:1;19:15;43:14;57:19; 61:19	wiped (2) 14:17;76:12	10 (12) 18:17;23:16;35:12;42:5, 6;57:3;64:20;79:10,17; 80:1,5,5
violated (1) 27:16	weapon (2) 18:20;73:12	within (11) 8:12;26:17;34:14;37:18; 39:11;53:19;55:13;71:18; 72:17;75:1;78:1	10:45 (1) 7:16
violating (1) 27:17	weapons (3) 28:14,15;35:4	without (3) 47:5;55:15;58:10	100 (2) 23:17;47:10
violation (1) 25:20	web (12) 16:6;21:1,3,5,17;48:21; 52:14;61:21;74:15,17; 75:16;79:9	witness (1) 5:7	101 (1) 66:19
violations (2) 27:14;51:15	website (16) 5:20;28:19;49:12,16; 50:20;52:4,8;53:12;55:8; 64:9;69:2;74:4,5;75:4; 76:21;79:21	witnessed (1) 71:14	108 (1) 76:18
violently (1) 59:8	websites (2) 23:16;74:6	witnesses (6) 5:10,16;13:15;17:16; 38:8;73:10	109 (3) 50:8;64:14,20
visitor (1) 75:3	week (2) 9:12;47:3	WMV (5) 72:18;78:12,15;79:1,15	11 (8) 18:21;24:14;28:6;35:19; 57:18,20;70:21;71:1
visualize (1) 41:20	weekend (1) 7:4	words (6) 9:10;12:14;22:4;46:8; 56:21;61:3	110 (1) 64:14
vital (1) 24:5	weekly (1) 42:19	work (4) 12:8;32:17;45:4;81:10	112 (1) 66:19
void (1) 77:20	weeks (7) 8:12;16:8;46:19;47:5; 51:3;65:1;71:18	worked (4) 30:18;36:15,19;38:4	114 (1) 24:1
volume (1) 15:2	whenever (1) 22:1	working (1) 48:17	115 (1) 66:2
volumes (1) 33:7	wholesale (1) 8:14	world (11) 11:15;14:9,14;41:11; 48:21;52:10;58:4;60:1,6; 68:5;71:17	116 (1) 66:3
volumetxt (1) 54:1	Whyte (1) 4:6	Worldwide (4) 9:6;21:5,17;49:15	119 (1) 16:7
voluminous (2) 11:16;15:4	widely (1) 29:3	worth (1) 9:10	12 (3) 5:5;54:16,21
voluntarily (2) 26:15;27:11	WikiLeaks (102) 8:18;9:14;10:1,19,21; 11:2,3,8,10;12:13,16;14:16; 15:12;16:7;17:6;28:8;33:2, 8;45:18;46:6,14,14,21; 47:10,15,20;48:1,6,7,18; 49:3,11,18;50:11,15,19; 51:8,11;52:2,8,9;53:10,11, 21;55:4,7,17;56:8,11,12,20; 57:5,5;58:3,8,9,11,13,16,20; 59:10,21;60:1,4;61:9;62:2, 3,4,8,10,14,19;63:2,6,8,14, 17,18;64:2,5,8;65:15;66:8, 12;67:6,20;68:4,11,13,15, 20;69:1;70:17,20;71:4,8,17;	Y	12:00 (1) 70:10
vulnerability (1) 55:6		year (1) 43:1	123 (1) 56:18
vulnerable (1) 55:5		years (2) 23:16;68:7	127 (2) 54:1;55:19
W		yesterday (1) 6:13	128 (3) 79:2,5,18
waged (1) 28:3		York (1) 59:17	129 (2) 79:17,20
walk (1) 12:17		Z	13 (4) 33:20;35:12,20;36:8
wantonly (1)		zip (4) 72:17;78:20;79:13,15	130 (2) 17:1,2

1330 (2) 81:10,12	5:3,6,9		5:5;26:1
139 (1) 49:7	21 (1) 19:8	4	65 (1) 73:6
14 (4) 4:11;19:5;53:7;54:17	210 (3) 27:8;36:14;47:3	4 (2) 5:4;34:8	7
15 (12) 16:1,1;20:6;66:21;70:2,6; 71:6;72:2,11;75:9;76:1; 80:12	216 (1) 23:9	4,000 (1) 23:17	7 (12) 18:7;23:21;24:2,8,15; 26:3;34:18,21;51:4;54:8; 57:16;76:13
154 (1) 66:4	219 (1) 23:12	40 (2) 14:7;59:1	71 (1) 20:14
155 (1) 66:5	22 (1) 14:7	41 (1) 19:17	7-100.1 (1) 29:1
15-6 (1) 81:6	221 (1) 23:13	42 (1) 68:10	7-100.4 (1) 29:8
15-minute (2) 69:14;70:6	223 (1) 23:15	43 (2) 54:14;55:10	72 (1) 20:18
16 (1) 5:5	23 (6) 52:13;77:4,8,12;78:1,5	44 (1) 66:10	73 (1) 20:20
160 (1) 13:13	24 (4) 5:3;28:9;46:11;67:8	45 (2) 51:5,9	7-903 (1) 25:21
161 (3) 77:14,15,21	25 (6) 5:6,9;33:19,20;47:12; 49:19	46 (3) 51:6;66:11;71:4	8
17 (1) 66:4	250,000 (1) 62:20	470 (1) 67:2	8 (8) 5:5;18:12;35:3;65:5; 66:18;71:8;75:14,17
18 (2) 5:5;25:21	251,287 (1) 63:9	474 (1) 67:2	80 (2) 13:15;62:19
19 (2) 16:19;53:7	26 (2) 54:11;58:18	48 (1) 19:20	802 (1) 6:19
2	272 (1) 62:21	5	81 (7) 47:16,16,19;65:4,13,18; 74:2
2 (6) 5:5;24:3;34:2;57:13; 70:21;71:1	28 (6) 65:5,10,17,18,21;77:3	5 (8) 17:19;34:12;50:5;53:21; 54:7;59:9,14;68:9	84 (1) 51:1
20 (2) 49:5,18	283 (1) 66:6	51 (1) 22:20	85 (3) 53:1,5;54:15
2-0 (1) 28:13	29 (6) 46:18,18;65:5,17;66:10; 73:19	52 (3) 18:4;20:12;21:9	9
2000 (1) 70:18	2nd (1) 47:2	525-13 (1) 28:17	9 (6) 35:7;46:10;56:19;65:20; 66:2;73:20
2003 (1) 66:15	3	54 (1) 4:8	9:20 (1) 4:7
2007 (1) 59:2	3 (2) 34:4;55:10	58 (1) 77:21	91 (3) 74:14,17,21
2008 (8) 24:3;26:4;32:3;33:21; 35:12,20;36:8;52:13	30 (4) 54:11;58:14;65:5;66:10	59 (1) 27:1	917 (1) 6:12
2009 (34) 8:3;16:1,1,8;24:3;32:10; 46:9;47:11;54:12;59:2; 65:11,14,18;66:7,10,15; 67:4,4,8;71:6;72:1,3,9,12; 73:18,19,20,20;75:10;76:1, 19;77:1;80:11,12	31 (3) 14:18;19:12;76:10	6	99 (1) 52:15
2010 (26) 9:12;14:18;16:14;47:12; 48:16;49:5;51:4;53:7;54:8, 18;60:18;62:17;71:9;75:14, 17;76:10,11;77:3,4,8,12; 78:1,5;79:10,17;80:1	32 (3) 65:18,21;75:13	6 (3) 5:5;17:19;34:17	
2013 (3)	33 (1) 59:4	60 (1) 27:5	
	35 (3) 4:10;17:16;25:1	614 (2) 5:3,18	
	38 (1) 19:15	615 (1) 5:6	
	380-5 (1) 18:6	616 (2) 5:9,14	
	3C (2) 54:9,16	617 (1) 5:12	
	3rd (1) 47:2	63 (2) 50:20;66:11	
		641 (2)	